مجلس التعاون لدول الخليج العربية

الأمانة العامة



مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية
لعام (٢٠١٥م)

الجريمة الإلكترونية

في المجتمع الخليجي وكيفية مواجهتها

Cybercrimes in the Gulf

Society and How to Tackle Them

إعداد

مجمع البحوث والدراسات

أكاديمية السلطان قابوس لعلوم الشرطة

نزوى ـ سلطنة عمان

البحث الفائز بالمركز الأول في المسابقة

٢٠١٦م

شكر وتقدير

بسم الله الرحمن الرحيم، والحمدلله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين.

يشرفني بأن أتقدم بالشكر والتقدير للقيادة العامة للشرطة والجمارك الموقرة على الدعم المستمر والمتابعة الحثيثة للوصول بجهاز شرطة عُمان السلطانية إلى المكانة التي تليق به بين أقرانه من أجهزة الشرطة في العالم، وأن يكون حاضراً في منصات التتويج الأولى، وتحقيق النتائج المتقدمة في كافة المجالات الأكاديمية والعسكرية والرياضية والثقافية.

والشكر موصولاً لقيادة أكاديمية السلطان قابوس لعلوم الشرطة التي كانت الداعمة الأساسية في التوجيه والإرشاد لتحقيق المركز الأول في هذا البحث الأكاديمي .

كما نتقدم بالشكر إلى هيئة التحكيم التي اختارت هذا البحث من ضمن البحوث التي حصلت على المركز الأول وفاز بالمركز الأول على البحوث الأخرى كأشخاص إعتبارية.

كذلك لا يفوتنا أن نتقدم بالشكر والعرفان للأمانة العامة لدول مجلس التعاون الخليجي التي منحت الجائزة لمجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة نتيجة لفوزه بالمركز الأول للأشخاص الاعتبارية.

كما نتقدم بالشكر والتقدير أيضاً لكل من ساهم في إعداد وإنجاز هذا البحث تحت عنوان الجريمة الإلكترونية، والذي تم إعداده من قبل مجمع البحوث والدراسات ممثلاً في كل من :

المقدم / سعيد بن سالم البادي

المقدم / زايد بن حمد الجنيبي

الدكتور/ يوسف الشيخ يوسف حمزة

الدكتور / محمود أحمد العطاء

والله ولي التوفيق ، ، ،

مدير مجمع البحوث والدراسات

المحتويات

الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها

الملخص

تعد الجريمة الإلكترونية من أبرز وأخطر التحديات الأمنية التي تواجه كافة مجتمعات العالم في مجال استخدامات تقنية المعلومات والاتصالات على نطاق مؤسسات القطاع العام والخاص والأفراد. والجرائم الإلكترونية نوعان: الأول: الجرائم الموجهة ضد جهاز الحاسب الآلي أو أنظمة تقنية المعلومات والاتصالات، والنوع الثاني: تلك الجرائم التي يكون فيها الحاسب الآلي وسيلة لارتكاب جرائم الاحتيال وسرقة الهويات وبطاقات الائتمان والأرصدة المالية والتزوير والاختلاس وسرقة حقوق الملكية الفكرية والإبتزاز والسلوك الانحرافي والاستغلال الجنسي للأطفال، إضافة إلى الترويج للأفكار المتطرفة ودعم وتمويل الإرهاب.

ظلت معدلات الجريمة الإلكترونية تتصاعد منذ عقد التسعينات وتضاعفت الجرائم وخسائرها المالية بعد أن بلغ عدد مستخدمي الإنترنت ٤٠٪ من سكان العالم في عام ٢٠١٤ وقدرت الخسائر المالية – ٤٥٠ مليار دولار وعدد الضحايا ٥٥٦ مليون، وأصبحت الجريمة الإلكترونية مهددا حقيقياً لأمن المعلومات ومصدر خطورة على الأمن القومي وعلى الأمن والسلم الدوليين.

تناولت الدراسة الموضوع في خمسة مباحث، إضافة إلى استراتيجية موحدة (مقترحة) منفصلة وذلك كما يلي:

المبحث الأول: ماهية الجريمة الإلكترونية وتطورها وأسبابها، وتناول هذا المبحث تعريفات الجريمة الإلكترونية ونشأتها وأنواعها وتطوراتها وآثارها.

المبحث الثاني: واقع الجريمة الإلكترونية وحجم الخسائر عام ٢٠١٣ دوليا وفي دول مجلس التعاون لدول الخليج العربية.

المبحث الثالث: التعاون الدولي والإقليمي في مواجهة الجريمة الإلكترونية في هذا المبحث تم تسليط الضوء على مبادرات نشأة الجهود الدولية التي أسفرت عن اتفاقية مجلس أوربا لمواجهة الجريمة الإلكترونية عام ٢٠٠١ وتواصلت الجهود الدولية والإقليمية المكثفة في المؤتمرات والندوات لإيجاد المعالجات والحلول لهذه الظاهرة.

المبحث الرابع: المراكز والآليات الأخرى الوطنية والإقليمية والدولية ودورها في حماية الأمن السيبراني، بصفة خاصة ومراكز فرق الاستجابة لطوارئ الحاسب الآلي (CERTS).

المبحث الخامس: مدى تأثير برامج التواصل الاجتماعي على مجتمع دول مجلس التعاون لدول الخليج العربية.

الاستراتيجية: استراتيجية موحدة لمواجهة الجريمة الإلكترونية في دول مجلس التعاون لدول الخليج العربية.

الخاتمة: توصلت الدراسة إلى نتائج واقعية وقدَّمت مجموعة من التوصيات البناءة.

Combating Cybercrime in Gulf Society

Abstract

Cybercrime is the most significant and dangerous security challenges facing all global societies in the field of information and communication technology , affecting all through public and private corroborations and individuals.

There are two types of Cybercrime: First: Crimes against computer devises or information and communication systems. Second: Crimes committed by using computer such as: fraud, credit card theft, forgery, embezzlement, blackmailing, hackering, cyber attack, theft of intellectual property rights, children sexual abuse, promotion of fanatic believes, support and financing of terrorism.

Rate of cybercrime is continually increasing since the nineteenth of the past century, and the financial losses of the crime has been doubled after users of internet had become 40% of the world population on 2013. Financial global losses estimated on 2013 was 450 billion dollar , number of victims was 556 million, and cybercrime now is the major and real threat to information security and source of danger to national security and international security and peace.

This study addresses the subject in five sub-chapters plus separated unified strategy for combating cybercrime in Gulf Cooperation Council Countries as follows:

Sub- chapter one: Identification of Cybercrime Development and Reasons:

This sub-chapter reviews definitions of cybercrime, first recognition of the crime, types and development.

Sub-chapter two: Current status of Cybercrime and amount of Losses Internationally and in the Cooperation Council of the Arab States of the Gulf.

Sub-chapter three: International Cooperation Combating Cybercrime:

This sub-chapter highlighted the initiatives of establishing international efforts that resulted the Council of Europe Convention on Cybercrime 2001, international and regional intensive efforts continued, conferences and symposiums seeking for solutions for this phenomenon.

Sub-chapter four: National, Regional, and International Centers and other mechanism, and it's role in protection of cyber security, especially Computer Emergency Response Teams (CERTs).

Sub-chapter Five: Effect of social networking software on Gulf Cooperation Council Countries (GCCC)

Strategy: Unified Strategy for combating Cybercrime in the Gulf Cooperation Council Countries (GCCC).

Conclusion: Convenient results where reached and collection of recommendations where provided.

المقـــدمـــة

اعتباراً لطبيعة الجريمة الإلكترونية العابرة للحدود وإمكانية ارتكابها من أي مكان في العالم لأحداث نتائجها في مكان آخر، وسرعة وسهولة إخفاء أدلتها، هذا التداخل في دوائر الاختصاص المكاني لمباشرة الإجراءات القانونية، إضافة إلى تعقيدات التحقيق فيها وضبط أدلتها ومرتكبيها، كل ذلك يجعل دراستها ومواجهتها في المجتمع الخليجي أو غيره من المجتمعات أمراً لا ينفصل عن التعرف بشكل عام على ماهيتها ومفهومها وأسبابها وتطوراتها ودوافعها وآثارها والجهود الدولية والإقليمية لمواجهتها والحد منها، فهي مشكلة عالمية تتأثر بها منطقة الخليج العربي بقدر معين مثل بقية أقاليم ودول العالم. وسوف نتناول ذلك بالقدر المناسب من التفصيل.

فالجريمة الإلكترونية نوعان: الأول: الجرائم الموجهة ضد جهاز الحاسب الآلي أو أنظمة تقنية المعلومات والاتصالات الأخرى بقصد اتلافها أو تدميرها أو تعطيلها, النوع الثاني: الجرائم التي يكون فيها الحاسب الآلي وسيلة ارتكاب جرائم الاحتيال وسرقة الهويات وبطاقات الائتمان والأرصدة المالية والتزوير والاختلاس وسرقة حقوق الملكية الفكرية والابتزاز والسلوك الانحرافي والاستغلال الجنسي للأطفال.

وقد مرت الجريمة الإلكترونية Cybercrime في تطورها بعدة مراحل منذ رصدها في الإحصائيات لأول مرة فالفترة من ١٩٧١ إلى ١٩٩٠ تضمنت ابرز الجرائم التي تم رصدها وضبطها على نطاق العالم وهي قليلة جدا ويتراوح عددها بين جريمة واحدة إلى ثلاثة في العام , وأشهرها في عام ١٩٨٨ عندما تم استخدام الحاسب الآلي لسرقة ٧٠ مليون دولار من بنك شيكاغو الوطني الأولFirst National Bank of Chicago [١]. وفي ذات العام ١٩٨٨ تم لأول مرة تكوين فريق طوارئ الحاسب الآلي[٢] (CERT) في معهد هندسة البرمجيات بجامعة كارنيجي ميلون الأمريكية لمواجهة الجريمة الالكترونية بأشكالها المختلفة.

وفي عام ١٩٨٩ تبنت اللجنة الوزارية لمجلس أوربا التوصية رقم ٩ (٨٩) R الخاصة

١ أنظر المصدر التالي: WAVEFRONT. Consulting Group. Certified Information Security Consults . Brief History of Cybercrime. 2012 ; www.warefrontcg.com أنظر الملحق رقم (٢) ص أ–ك.

٢ Computer Emergency Response Team (CERT) Created in1988at Carnegie Ireton University .USA
ويعد هذا الفريق النواة الأولى للفرق المماثلة المنتشرة في جميع أنحاء العالم ومن بينها دول مجلس التعاون لدول الخليج العربية.

بمواجهة جرائم الحاسب الآلي[٣].

وتميزت الفترة من ١٩٧١ إلى١٩٩٠ بعدم الانتشار الواسع لاستخدام الحاسب الآلي والإنترنت وقلة عدد المستخدمين بالمقارنة مع السنين التالية.

في عقد التسعينات ارتفع معدل الجرائم الالكترونية نسبيا وكان أشهرها عام ١٩٩٤عندما كان عدد مستخدمي الانترنت حول العالم ٢٥,٤٥٤,٥٩٠ مليار[٤] اخترق طالب أمريكي عمره ١٦ سنة اسم الشهرة data stream (نهر البيانات) أجهزة الكمبيوتر في معهد أبحاث الطاقة الكوري Korean Atomic Research Institute وكالة ناساNASA ووكالات حكومية أمريكية أخرى وتم اعتقاله في انجلترا[٥]. وفي عام ١٩٩٥ تمكنت عصابة روسية محترفة من سرقة عشرة ملايين دولار من مصرف سيتي بنك City bank باستخدام الكمبيوتر وتحويلها إلى حسابات في فنلندة واسرائيل[٦], وفي ذلك العام -١٩٩٥- وصل عدد المستخدمين للإنترنت إلى ٤٤,٨٣٨,٩٠٠ بزيادة ٧٦,٢٪ عن العام السابق.[٧]

وتميز عقد التسعينات بأن عددا من الحكومات أصدرت تشريعات لمواجهة الجريمة الالكترونية Cybercrime وتوفرت بعض إحصائيات استخدام الإنترنت منذ العام ١٩٩٣ حيث كان عدد المستخدمين في ذلك العام ١٤,١٦١,٥٧٠ فقط وكان عدد سكان العالم ٥,٥٧٨,٨٦٥,١١ مليار وتضاعف عدد المستخدمين ليصل عام ١٩٩٩ إلى ٢٨٠,٨٦٦,٦٧٠ مليون بعد أن وصل عدد سكان العالم إلى ٦,٠٥,٤٧٨,٠١٠ مليار نسمة [٨] في ذلك العام.

وحفلت الفترة من عام ٢٠٠٠ إلى ٢٠١٤ بتطورات كثيرة ومتسارعة في ارتفاع أعداد مستخدمي الإنترنت وارتفاع معدلات الجرائم وضخامة الخسائر المالية وتواصل الجهود الدولية والإقليمية والوطنية لمواجهة الجريمة الالكترونية. فقد أصدر مجلس أوربا في عام ٢٠٠١ اتفاقية

---

٣ Council of Europe (committee of Ministers) 1989.

٤ Number of Internet Users (2014) Internet Live stats

٥ المصدر: Number of Internet Users (2014) Internet Live stats
الموقع: www.Intemetliveststs internet-users-

٦ المرجع السابق ، ملحق رقم (٣).

٧ أنظر المرجع السابق، Number of Internet Users (2014) ملحق رقم (٣) .

٨ المرجع السابق ، ملحق رقم (٣)

مجلس أوربا للجريمة الإلكترونية[٩] Council of Europe Convention on Cybercrime وكان للتأخير في التصديق على الاتفاقية وإنفاذها آثار سلبية بالغة أهمها استفحال الجريمة الإلكترونية وضخامة الخسائر المادية و تعقيدات المواجهة.

وفي عام ٢٠٠٢ بلغ عدد سكان العالم ٦,٢٨٠,٨٥٣,٨٢٠ ووصل مستخدمي الانترنت إلى ٦٦٢,٦٦٣,٦٠٠ بزيادة ٣٢٪ عن العام ٢٠٠١[١٠] وأصدرت منظمة التعاون الاقتصادي والتنمية (OECD)[١١] مرشدا لأمن نظم المعلومات والشبكات Guidelines for the Security of Information Systems and Networks

ورغم التصاعد المستمر في أعداد المستخدمين للإنترنت والجرائم الالكترونية منذ بداية الألفية الثالثة, لم تتفاعل حكومات العالم بالقدر المطلوب لحماية الأمن السيبراني، علما بأن كل المجتمعات حول العالم صارت تعتمد بشكل أساسي على شبكات الحاسب الآلي في القطاع العام و الخاص وعلى مستوى الأفراد, إلا انه في السنين القليلة الماضية أصبحت حماية أمن المعلومات والاتصالات والشبكات ومواجهة الجريمة الإلكترونية تشكل أولوية في سياسات العديد من الحكومات.

بعد الهجمات الإلكترونية الشهيرة على دولة استونيا عام ٢٠٠٧ Cyber attacks

---

٩ وقعت على الاتفاقية في تاريخ إجازتها ٢٠٠١/١١/٢٣ في مؤتمر بودابست ٢٦ دولة من الدول الأعضاء، في مجلس أوربا البالغ عددها ٤٧ دولة بالإضافة إلى أربعة دول غير أعضاء في مجلس أوربا وهي: الولايات المتحدة الأمريكية، اليابان، كندا، جنوب أفريقيا وذلك وفقاً لنص المادة (٣٧) من الاتفاقية التي تجيز انضمام الدول غير الأعضاء في مجلس أوربا، وفي آخر إحصائية بتاريخ ٢٠١٤/١٠/٥ وقعت على الاتفاقية ٤٥ من الدول الأعضاء من أصل ٤٧ دولة وبقيت دولتان لم توقعا هما روسيا وسان مارينو. ويلاحظ تأخر الدول الأوربية الغربية الأعضاء في مجلس أوربا كثيراً في التصديق على الاتفاقية وإنفاذها، وكشف التحليل الذي أجريناه أن ١٠ دول أعضاء بنسبة ٢٣,٢٥٪ قد وقعت على الاتفاقية في الفترة من ٢٠٠٤ إلى ٢٠٠٥ وأن ١٣ دولة بنسبة ٣٠,٤٪ صدقت على الاتفاقية وأدخلتها حيز النفاذ في الفترة من ٢٠٠٦ إلى ٢٠٠٩، و١٣ دولة صدقت على الاتفاقية وادخلتها حيز النفاذ في الفترة من ٢٠١٠ إلى ٢٠١٤ بنسبة ٣٠,٢٪ ، أما الدول الأربعة غير الأعضاء في مجلس أوربا والتي وقعت على الاتفاقية عند إجازتها بتاريخ ٢٠٠١/١١/٢٣، فقد صدقت عليها الولايات المتحدة الأمريكية في ٢٠٠٦/٩/٢٩ وانفاذها في ٢٠٠٧/١/١ وصدقت عليها اليابان في ٢٠١٢/٧/٣ وانفاذها في ٢٠١٣/٣/١ وصدقت عليها كندا في ٢٠١٢/١١/٣٠ وانفاذها في ٢٠١٣/٣/١ أما استراليا فقد صدقت على الاتفاقية في ٢٠١٢/١١/٣٠ وكان انفاذها في ٢٠١٣/٣/١.

١٠ أنظر المصدر السابق: Number of Internet Users (2014) Internet Live stats

١١ منظمة التعاون الاقتصادي والتنمية هي منظمة اقتصادية دولية تأسست عام ١٩٦١ من الدول الأوروبية وأمريكا وكندا وتضم في عضويتها ٣٤ دولة منهم ٢١ من أصل ٢٨ دولة هم أعضاء الاتحاد الأوربي ماعدا بلغاريا، كرواتيا، قبرص، لاتفيا، استونيا، مالطا، رومانيا.

Orgnization for Economic Co-operation and Development (OECD).

on Estonia انتبهت الكثير من الدول لهذا الخطر الذي يدمر البنيات التحتية للمعلومات وتقنية الاتصالات والشبكات ويعطل كل المرافق الحيوية الاقتصادية والمالية والتعليمية والصحية والاجتماعية في القطاع العام أو الخاص.[١٢] وتجدر الإشارة إلى أن عدد سكان العالم عام ٢٠٠٧ الذي حدثت فيه الهجمات الإلكترونية على جمهورية استونيا- قد بلغ ٦,٦٧٣,١٠٥,٩٤٠ نسمة وبلغ عدد مستخدمي الإنترنت ١,٣٧٣,٠٤٠,٥٤٢ بزيادة ١٨,٦٪ عن العام السابق , وفي عام ٢٠٠٧ بلغت تقديرات خسائر الجريمة الإلكترونية ٣٢٠مليون دولار. وبدأت الدول في التفكير الجاد والخطوات التنفيذية لإعداد استراتيجيات الأمن السيبراني Cyber Security Strategies وبالفعل تم انجاز عدد من الاستراتيجيات على نطاق العالم، ثم نشرها وفي مقدمتها استراتيجيات ١٨ دولة من دول الاتحاد الأوربي البالغ عددها ٢٨ دولة. واستراتيجيات ١٨دولة أخرى حول العالم من بينها الولايات المتحدة الأمرِيكية واستراليا وكندا والهند واليابان.

ويلاحظ أن دول الشرق الأوسط ليست من بين الدول التي أعدت استراتيجيات - منشورة ومعلومة للمجتمع الدولي- لمواجهة الجريمة الإلكترونية وحماية الأمن السيبراني, وسوف نستخلص من بعض الاستراتيجيات المذكورة المبادئ والمرتكزات التي يعتمد عليها مشروع استراتيجية دول مجلس التعاون لدول الخليج العربية المقترح[١٣].

احصائيات استخدام الانترنت:

وتأكيداً لأهمية وضرورة إعداد استراتيجية خاصة بدول مجلس التعاون لدول الخليج العربية لمواجهة الجريمة الإلكترونية، نستعرض فيما يلي بإيجاز آخر الإحصائيات لعام ٢٠١٤م عن استخدام الانترنت حول العالم وبصفة خاصة في دول الخليج العربية إضافة الى واقع الجريمة الإلكترونية Cybercrime وما نتج عنها من خسائر مادية ضخمة للاقتصاد العالمي

---

١٢ بدأت الهجمات الإلكترونية على استونيا Cyberia attacks يوم ٢٧ إبريل ٢٠٠٧ إلى ١٧ مايو ٢٠٠٧ وشمل الهجوم مواقع المنظمات والمؤسسات والبرلمان والمصارف والوزارات والمؤسسات الصحفية وأجهزة البث الإذاعي والتلفزيوني، وعلى خلفية الخلافات بين روسيا واستونيا اتهمت الأخيرة روسيا بتدبير هذه الهجمات الإلكترونية وثار جدل كثير حول هذه الاتهامات التي رفضتها روسيا، ويعد الهجوم الإلكتروني على استونيا ثاني أكبر حادثة في هذا المجال على المستوى الدولي بعد الهجمات التي استهدفت أنظمة الكمبيوتر بالولايات المتحدة الأمريكية عام ٢٠٠٣ واستمرت لمدة ثلاث سنوات وأطلقت عليها الحكومة الأمريكية الفيدرالية "مطر التيتان" Titan Rain واتهمت فيها الصين ولكن ظل الفاعل مجهول.

١٣ أنظر الملحق رقم (١) ص أ-م ، تحت عنوان استراتيجية موحدة لمواجهة الجريمة الإلكترونية في دول مجلس التعاون لدول الخليج العربية.

global economy. تقدر سنويا بأكثر من ٤٤٥ مليار دولار.

لقد بلغ عدد سكان العالم في ١ يوليو ٢٠١٤م ٧,٢٤٣,٧٨٤,١٢١ وبلغ عدد مستخدمي الإنترنت حول العالم يوم ٣٠ نوفمبر ٢٠١٤م الساعة ٥:١٩/ ٣,٠١٨,٦٢٧,٣٥٢ مليار – أي حوالي ٣ مليار نسمة. وبلغ عدد المواقع الإلكترونية في نفس اليوم ١,١٣٠,٦٤٤,٦٢٨ وعدد البريد الإلكتروني الذي تم إرساله في نفس اليوم ١٦٩,٢٦٠,٠٠٠ مليون ، أما في دول مجلس التعاون الخليجي لدول الخليج العربية، أفادت الإحصائية في ١ يوليو ٢٠١٤م أن عدد مستخدمي الإنترنت في المملكة العربية السعودية ١٧,٣٩٧,١٧٩ مليون بنسبة ٥٩,٢٤٪ من عدد السكان البالغ ٢٩,٣٦٨,٤٢٨ مليون والترتيب العالمي رقم (٣٠) ، وعدد المستخدمين في دولة الإمارات العربية المتحدة ٨,٨٠٧,٢٢٦ مليون بنسبة ٩٣,٢٤٪ من عدد السكان البالغ ٩,٤٤٥,٦٢٤ مليون والترتيب العالمي رقم (٤٦). عدد مستخدمي الإنترنت في الكويت ٤,٠٢٢,٠١٠ مليون بنسبة ٨٦,٨٦٪ من عدد السكان البالغ ٣,٤٧٩,٣٧١ مليون والترتيب العالمي رقم (٨٤) ، وعدد مستخدمي الإنترنت في سلطنة عمان ٢,٥٨٤,٣١٦ مليون بنسبة ٦٥,٨٢٪ من عدد السكان البالغ ٣,٩٢٦,٤٩٢ مليون والترتيب العالمي رقم (٨٩). عدد مستخدمين الإنترنت في دولة قطر ٢,٢٦٧,٩١٦ مليون ، بنسبة ٩٦,٦٥ ٪ من عدد السكان والترتيب العالمي رقم ٩٣، أما مملكة البحرين فعدد مستخدمي الإنترنت فيها ١,٢٩٧,٥٠٠ مليون بنسبة ٩٦,٥٣٪ من عدد السكان البالغ ١,٣٤٤,٠٠٠ مليون والترتيب العالمي رقم ١١٥.[١٤]

مشكلة البحث:

تكمن مشكلة البحث في تفاقم الجريمة الإلكترونية وتعدد أنواعها وازدياد حجم خسائرها وأضرارها بحيث أصبحت مهدداً حقيقياً لأمن المعلومات في كافة المجالات العامة والحيوية بالقطاع العام والخاص والأفراد، بل مصدر خطورة على الأمن القومي وعلى السلم والأمن الدوليين بسبب استخدام الإنترنت في النشاطات الإرهابية.

وتشكل العوامل التالية مشكلة البحث وتجعلها اكثر تعقيدا:

– الرغبة في جمع المعلومات وتعلمها ولو بطرق غير مشروعة.

–الاستيلاء على المعلومات المحفوظة في الحاسب الالي أو المنقولة عبر شبكة الانترنت أو

١٤ المرجع السابق: .Number of Internet Users (2014) – Internet Live Stats وأنظر الإحصائيات في الملحق رقم (٤) ص ب.

تغييرها أو حذفها أو الغائها نهائيا من النظام.

- قهر النظام وإثبات التفوق على وسائل التقنية وإثبات قدرة الجاني وتفوقه بكسر الحواجز الأمنية للأنظمة الالكترونية واختراقها.
- إلحاق الأذى بأشخاص أو جهات إعتبارية.
- تحقيق أرباح او مكاسب مادية.
- تهديد الأمن القومي العسكري والاقتصادي والاجتماعي.
- إرتفاع معدلات الجرائم الالكترونية عالميا وفي دول الخليج العربي.
- صعوبة مكافحة الجرائم الالكترونية على المستوى الوطني والدولي بسبب سهولة إخفاء معالم الجريمة وصعوبة الحصول على الدليل المادي.
- الاستخدامات السلبية لشبكات التواصل الاجتماعي ، ويشمل ذالك بث الافكار الهدامة والمنحرفة وعرض المواد الاباحية الفاضحة والاحتيال والابتزاز والتزوير وانتهاك الحقوق الخاصة والاستغلال الجنسي للأطفال .
- تعد الآثار السلبية لاستخدام مواقع التواصل الاجتماعي أحد مكونات مشكلة البحث لاسهامها في نشر الفساد بالاستلاب الثقافي والتاثير على القيم الدينية والاخلاقية.

و يزدار حجم الجريمة الإلكترونية بازدياد عدد مستخدمي الإنترنت حول العالم ،وبالاطلاع على الموقع الإلكتروني للرصد المستمر على مدار الثانية لمستخدمي الإنترنت يوم ٥ يناير ٢٠١٥م الساعة س٢٠ دق ١٠ ث ١٥ كان عدد المستخدمين ٣,٠٤١,٣٦٥,٨٠٠ وأن حوالي ٤٠٪ من سكان العالم لديهم اتصال بالإنترنت في هذا اليوم، وكانت هذه النسبة بلغت ١٪ فقط في عام ١٩٩٥ وأن عدد مستخدمي الإنترنت ازداد عشرة مرات في الفترة من ١٩٩٩– ٢٠١٣، وكان الوصول إلى المليار الأول من المستخدمين عام ٢٠٠٥ والمليار الثاني عام ٢٠١٠ والمليار الثالث في الربع الأخير من عام ٢٠١٤.[١٥] ومن المؤكد أن هذا الارتفاع الهائل والمتسارع في أعداد مستخدمي الإنترنت ينعكس سلباً على ارتفاع أعداد مرتكبي جرائم الإنترنت وزيارة حجمها. وفي عام ٢٠١٣ قدرت خسائر النشاطات الاقتصادية العالمية بأكثر من ٤٥٠ مليار دولار[١٦] وبلغ عدد ضحايا الجريمة الإلكترونية ٥٥٦ مليون بواقع ١,٥ مليون

---

١٥ المصدر: Internet Live Stats. Internet Users وأنظر الملحق رقم (٣) ص أ–ط.
http;// www.internetlivestats.com

١٦ Net Losses; Estimating the Global cost of Cybercrime. Economic Impact of Cybercrime11. Report Summary. Intel Security. 2014. www.macfee.com وأنظر الملحق رقم (٤) ص ب.

ضحية في اليوم وبمعدل ١٨ ضحية كل ثانية، وأن أكثر من ٢٣٢,٤ مليون بطاقة هوية تمت سرقة بياناتها وأن أكثر من ٦٠٠,٠٠٠ حساب في الفيس بوك يتم الاشتباه فيها ومراقبتها يومياً.[١٧]

أهمية الدراسة:

تكسب الدراسة أهميتها من أهمية التحديات الأمنية والتقنية والقانونية المصاحبة لاستخدامات تقنية المعلومات والحاسب الآلي والإنترنت ومن خطورة الوضع الراهن للجريمة الإلكترونية على البنيات التحتية لأنظمة تقنية المعلومات والاتصالات وتهديد الاختراقات والهجمات المستمرة لكل المصالح على نطاق مؤسسات القطاع العام والخاص والأفراد، مما يحتم ضرورة إيجاد المعالجات والحلول العلمية والعملية للحماية من الجريمة الإلكترونية والحد من إرتفاع معدلاتها وآثارها التي أكدتها كل الدراسات المتخصصة التي دقت ناقوس الخطر.

حدود الدراسة:

نظرا لان الجريمة الالكترونية عابرة للحدود والقارات بحيث يمك ارتكابها في اي مكان في العالم وتنتج اثارها واضرارها في بلد آخر، لذلك تتسع حدود الدراسة لتشمل اوضاع هذه الضاهره حول العالم ودور التعاون الدولي والاقليمي في مكافحتها وكشفها وضبط مرتكبيها .

أهداف الدراسة.

تتمثل أهداف الدراسة في الآتي:

١. إبراز الواقع الحالي للجريمة الإلكترونية وحجمها وأساليبها وأسبابها وآثارها وتطورها وخسائرها على نطاق العالم بشكل عام وفي منطقة الخليج العربي بصفة خاصة.
٢. عرض متطلبات رفع كفاءة وفاعلية أساليب ووسائل مواجهة الجريمة الإلكترونية دولياً وفي دول مجلس التعاون لدول الخليج العربية من حيث التقنيات المتطورة والكفاءات البشرية المؤهلة وإنشاء مراكز الاستجابة لطوارئ الحاسب الآلي وإعداد البرامج التنفيذية للحد من الجريمة الإلكترونية برصد التهديدات والمخاطر والتحذير المبكر منها، إضافة إلى تشريعات مواكبة ونظام عدالة جنائية على قدر عالي من التأهيل والكفاءة.
٣. التأكيد على ضرورة التعاون الإقليمي الدولي لمواجهة الجريمة الإلكترونية.
٤. وضع استراتيجية موحدة لدول مجلس التعاون لدول الخليج العربية لمواجهة الجريمة الإلكترونية

١٧ أنظر المرجع التالي: Cybercrime statisics and Trends.2014 Report.www.go-qulf.com

تستند على الأهداف والمبادئ الأساسية التي اتفقت عليها استراتيجيات دول العالم التي تم إعدادها في الفترة من ٢٠٠٨ إلى ٢٠١٣.

فروض الدراسة:

- انتشار الجريمةالالكترونية في دول مجلس التعاون لكونها جريمة عابرة للحدود..
-الوضع الاقتصادي والمالي والتجاري لدول الخليج يشكل بيئة مغرية للجريمة الالكترونية.
-الارتفاع الكبير والمتلاحق في أعداد مستخدمي الانترنت يؤدي إلى ارتفاع معدلات الجريمة الالكترونية وتعدد أشكالها وأنماطها .
-إتفاع خسائر وأضرار الجريمة الالكترونية يرتبط بازدياد اعداد مستخدمي الانترنت لأغراض غير مشروعة.
-تواجه الأجهزة الأمنيه والاجهزة المختصة الاخرى صعوبات على المستوى الدولي و الإقليمي في التعامل مع الجريمة الالكترونيه .
-من الممكن الوقاية من الجريمة الالكترونية ومكافحتها بوسائل عديدة.
-تفشي الاستخدامات السلبية لشبكات التواصل الاجتماعي.
-تأكيد الدور الهام للتعاون الدولي و الإقليمي لمواجهت الجريمة الالكترونية.
-احتمالات تاثير شبكات التواصل الاجتماعي على مجتمع دول مجلس التعاون ايجابا وسلبا.
-تأكيد دور المراكز التقنية والآليات الأخرى الوطنية والإقليمية والدولية في إعداد البرامج التنفيذية وحماية الأمن السيبراني.
-أهمية إعداد إستراتيجية موحده لمواجهة الجريمة الكترونية في دول مجلس التعاون لدول الخليج العربي.

تقوم الدراسة باختبار كل الفرضيات السالف ذكرها للوصول الى تفسير ظاهرة الجريمة الالكترونية في المجتمع الخليجي وتفسير العلاقة بين المتغيرات مما يسهم في تحديد نتائج البحث.

تساؤلات الدراسة:

لتنفيذ عمليات المواجهة التقنية والتشريعية والأمنية للجريمة الإلكترونية على النطاق الدولي والإقليمي، تقدم الدراسة الإجابة على التساؤلات حول الموضوعات التالية:

- التعريف بماهية الجريمة الإلكترونية وأسبابها وآثارها.

- توضيح حجم ظاهرة الجريمة الإلكترونية بارتفاع معدلاتها وخسائرها وتهديداتها عالمياً وفي دول مجلس التعاون لدول الخليج العربية بصفة خاصة.
- إبراز الصعوبات والتعقيدات وأوجه القصور بشأن التصدي للجريمة الإلكترونية وكشف أدلتها وملاحقة مرتكبيها وضبطهم.
- بيان كيفية إعداد البرامج التنفيذية لمواجهة الجريمة الإلكترونية وأساليب تقييم هذا البرامج.
- مدى تأثير برامج التواصل الاجتماعي على مجتمع دول مجلس التعاون لدول الخليج العربية.
- مدى إمكانية تضامن الجهود الدولية والإقليمية لمواجهة الجريمة الإلكترونية.

الدراسات السابقة:

استنند هذا البحث بشكل أساسي على الدراسات السابقة الحديثة التي أعدتها مراكز البحوث والدراسات حول العالم وتناولت تطورات الجريمة الالكترونية عالميا وحجمها وإحصاءاتها ومعدلات إرتفاعها وخسائرها المادية وأضرارها الاجتماعية والأخلاقية والاقتصادية، وقد تم إدراج هذه الدراسات كمصادر في قائمة المراجع .

اما الدراسات العربية التي تناولت موضوع البحث بالتحديد تكاد ان تكون نادره ومع ذلك تمت الاستفادة في البحث من دراسات عربية ذات صلة بالموضوع أشرنا إليها في قائمة المراجع باللغة العربية.

منهج الدراسة:

المنهج الوصفي التحليلي:

يتم من خلال هذا المنهج تحديد ماهية ظاهرة الجريمة الإلكترونية وطبيعتها وأسبابها واتجاهاتها وآثارها والعلاقة بين المتغيرات وتحليل الروابط وسبر أغوار مشكلة البحث والتعرف على حقيقتها وحجمها وأفضل الوسائل والمعالجات لمواجهتها وايجاد الحلول لها.

خطة البحث: تم تقسيم الدراسة إلى خمسة مباحث كما يلي:

المبحث الأول: ماهية الجريمة الإلكترونية وتطورها وأسبابها.

المبحث الثاني: واقع الجريمة الإلكترونية وأساليب مواجهتها.

المبحث الثالث: برامج التواصل الاجتماعي ومدى تأثيرها على مجتمع دول مجلس التعاون لدول الخليج العربية.

المبحث الرابع: التعاون الدولي والاقليمي لمواجهة الجريمة الإلكترونية.

المبحث الخامس: المراكز التقنية والآليات الاخرى الوطنية والاقليمية ودورها في حماية الأمن السيبراني.

الخاتمة: وتشمل: النتائج- التوصيات.

بالإضافة إلى استراتيجية منفصلة تحت العنوان التالي: استراتيجية موحدة لمواجهة الجريمة الإلكترونية في دول مجلس التعاون لدول الخليج العربية. (مرفقة).

المبحث الأول
ماهية الجريمة الإلكترونية وتطورها وأسبابها وآثارها

لا شك أن التقدم الحضاري الذي اجتاح العالم في العصر الحديث أثّر في كافة مناحي الحياة الانسانية من سلوكيات وغيرها وقد طال هذا التأثير نوعية الجريمة والمجرم وأصبح ملموساً لدى كل المختصين والمهتمين بعلم الإجرام والمجرمين.

ومن نتائج التطور الحضاري الذي اجتاح العالم الحديث تقنية المعلومات التي تعتبر العامل الأساسي الذي أحدث ثورة هائلة في مجال الاتصالات واستخدامات الحاسب الآلي والإنترنت للأغراض المختلفة، وفي نفس الوقت ساهمت في إنتاج وتطوير كثير من السلوكيات التي تعتبر إجراما وفقاً لقوانين وقواعد التجريم ولا شك أن لها الأثر البالغ على حياة أفراد مجتمعات العالم وعلى القطاع العام والخاص.

وعلى ما تقدم سنحاول التعرف على هذا النوع من الإجرام وذلك من خلال البحث في ماهية الجريمة الإلكترونية وتطورها.[١٨]

نتناول موضوعات هذا المبحث في مطلبين:

المطلب الأول: ماهية الجريمة الإلكترونية وتطورها.

المطلب الثاني: أسباب الجريمة الإلكترونية وآثارها.

المطلب الأول
ماهية الجريمة الالكترونية وتطورها

نقسم هذا المطلب إلى فرعين:

الفرع الأول: ماهية الجريمة الإلكترونية.

الفرع الثاني: تطور الجريمة الإلكترونية.

---

١٨ - http:llhussain-algafri-blogspot.com

الفرع الاول
ماهية الجريمة الالكترونية

أولاً: تعريف الجريمة الالكترونية في الفقه.

لم يتفق الفقه الجنائي على تسمية موحدة للجريمة الإلكترونية، إذ يطلق عليها البعض الجريمة الإلكترونية وهناك من يسميها الجريمة المعلوماتية، ويذهب أخرون إلى تسميتها بجرائم إساءة استخدام تكنولوجيا المعلومات والاتصال ويطلق عليها آخرون مسمى جرائم الكمبيوتر والإنترنت.

وبما أن إيجاد تعريف للجريمة الإلكترونية كان محلاً لاجتهادات الفقهاء، فقد ذهبوا في ذلك مذاهب مختلفة ووضعوا تعريفات شتى وبالتالي فلا نجد تعريفاً محدداً للجريمة الإلكترونية. وهناك اختلاف بين الباحثين في تعريف الجريمة الإلكترونية، فمنهم من يتناول التعريف من الجانب التقني «فنياً» ومنهم من يتناوله من الزاوية القانونية. فالذين يتناولونه من الجانب التقني يذهبون الى القول بأن الجريمة المعلوماتية ما هي إلا «نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود».[١٩]

أما أنصار الاتجاه القانوني فيذهبون إلى أن تعريف الجرائم الإلكترونية يتطلب تعريف المفردات الضرورية المتعلقة بارتكاب جرائم الحاسب الآلي وهي «الحاسب الآلي . برنامج الحاسب الآلي . البيانات . الممتلكات . الدخول . الخدمات .

الخدمات الحيوية» [٢٠]. وفريق آخر من الفقهاء أيضاً يعرف جريمة الحاسب الآلي « أو الجريمة الإلكترونية بأنها «الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الإنترنت [٢١].

ويرى أنصار الجانب الفقهي بأن هذه الجريمة تتسم بالسرعة وتطور وسائل ارتكابها وينعدم فيها العنف المادي ضد الإنسان بالمقارنة مع الجرائم التقليدية أثناء تنفيذها، وهي عابرة للحدود

---

١٩ د. محمد الامين البشري . التحقيق في جرائم الحاسب الآلي . بحث مقدم إلى مؤتمرات القانون والكمبيوتر والانترنت . كلية الحقوق والشريعة . جامعة الامارات ٢١ . مايو٢٠٠٥ . ص ٦ .

٢٠ د. عبدالفتاح بيومي حجازي . مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي . دار الفكر الجامعي . الإسكندرية ٢٠٠٦ . ص ٢٠ .

٢١ د. محمد عبدالرحيم سلطان العلماء . جرائم الإنترنت والاحتساب عليها . بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت . جامعة الامارات . مايو ٢٠٠٥ . ص ٥.

ومن سماتها أيضاً أن أدلتها سهلة الإتلاف. كما أن الجهات التي تتولى تعقبها والتحقيق فيها تواجه صعوبات وتعقيدات كثيرة وتنقصها أحياناً الخبرة وعدم كفاية القوانين الخاصة بمعالجتها. (٢٢)

وهناك من يأخذ على هذا التعريف قصوره في عدم الاشارة إلى بيئة وقوع الجريمة الإلكترونية وهي الشبكة العالمية للمعلومات «الإنترنت «كما هو الحال عند تعطيل الشبكة عن العمل أو العمل على إبطاء سرعتها أو إتلاف المواقع عليها (٢٣).

واتجاه آخر من الفقه يتخذ وسيلة ارتكاب الجريمة كأساس لوضع التعريف للجريمة الإلكترونية كما هو الحال عند الفقيه الألماني تاديمان الذي عرفها بأنها «هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي «(٢٤).

وفي نفس الاتجاه عرفت بأنها «الجرائم التي يكون قد وقع في مراحل إرتكابها بعض عمليات فعلية داخل نظام الحاسوب وبعبارة أخرى هي تلك الجرائم التي يكون دور الحاسوب فيها إيجابياً أكثر منه سلبياً» (٢٥). كذلك تعرف بأنها «كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دوراً لتمامه على أن يكون هذا الدور على قدر من الأهمية (٢٦).

وهناك اتجاه آخر من الفقه يركز على الجانب الموضوعي في تعريفه للجريمة الإلكترونية فيرى أن الجريمة الإلكترونية لا يكفي لإطلاق هذا الوصف عليها بمجرد استخدام الحاسب الآلي فيها ولكن يشترط أن يقع الفعل داخل نظام الحاسب الآلي لاحتسابها جريمة إلكترونية. (٢٧) ولذلك عرفوا الجريمة الإلكترونية بأنها « نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسب أو التي ترسل عن طريقه «، كما عرفوها بأنها «غش معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها «(٢٨).

---

٢٢ د. محمد عبدالرحيم سلطان العلماء. المرجع السابق. ص ٥.

٢٣ د. المدرس المساعد. عادل يوسف عبدالنبي الشكري. الجريمة المعلوماتية وأزمة الشريعة الجزائية، مركز دراسات الكوفة، ٢٠٠٨، ص ١١٢ -١١٣. htt;// www.iasj.net. 13-10-2015;1100

٢٤ د. المدرس المساعد. عادل يوسف عبدالنبي الشكري. المرجع السابق. ص ١١٣

٢٥ د. عبدالفتاح بيومي حجازي. المرجع السابق ص ٢٤ .

٢٦ د. نائلة عادل محمد فريد فودة. جرائم الحاسب الاقتصادية. دراسة نظرية تطبيقية ، دار النهضة العربية ، القاهرة ، ٢٠٠٤، ص٢٥ -٢٦.

٢٧ د. عبد الفتاح بيومي حجازي. المرجع السابق. ص٢٥.
://www.bayt.comptth ٢٠١٥/١/١ الوقت ١٦٣٤

٢٨ د. علي عبد القادر القهوجي. الحماية الجنائية لبرامج الحاسوب. دار الجامعة الجديدة للنشر. الإسكندرية ١٩٩٧. ص

وفريق أخر من الفقه يركز على الجانب المعرفي - لا على الوسيلة أو الموضوع - للجريمة الإلكترونية وذلك لكونها مرتبطة بالجوانب المعرفية الفنية أو المعرفة باستخدام الحاسب الألي ولذلك عرف أنصار هذا لاتجاه الجريمة الإلكترونية بأنها « أية جريمة يكون متطلباً لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب الآلي «كما عرفها الدكتور هشام فريد رستم بأنها « أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه».[٢٩]

كما عرفت في تفس الاتجاه بأنها (كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها».[٣٠] وقد أنتقد هذا التعريف حيث يرى منتقدوه بأنه يوسع من نطاق الجريمة الإلكترونية لأنه ساوى بين السلوك غير المشروع قانوناً والمعاقب عليه والسلوك الذي يستحق اللوم أخلاقيا فقط. [٣١]

ويرى جانب من الفقه أن الجرائم التي لها ارتباط بالمعلومات هي ذاتها التي تسمى الغش المعلوماتي وهذه يقصد بها كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية.[٣٢]

وقد عرفها الفقيه الفرنسي Masse بأنها "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح" [٣٣] وهي « كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها «[٣٤].

ثانياً: تعريف الجريمة الالكترونية في التشريعات الخليجية.

بدراسة الأنظمة والتشريعات الخليجية نجد تفاوتاً بينها، أي أن بعض هذه الأنظمة والتشريعات عرف الجريمة الالكترونية والبعض الآخر لم يتطرق لتعريفها مكتفياً بتسمية الأفعال التي يجرمها ووضع لها العقوبات التي يراها مناسبة لها.

فالمشرع القطري عرف الجريمة الالكترونية . في القانون رقم ١٤ لسنة ٢٠١٤م الصادر

---

٢٩ د. عبدالفتاح بيومي حجازي . المرجع السابق ص ٢٥.

٣٠ المدرس المساعد / عادل يوسف عبد النبي الشكري . المرجع السابق . ص ١١٣.

٣١ د. عبدالفتاح بيومي حجازي . المرجع السابق ص ٢٦.

٣٢ د. محمد سامي الشوا . ثورة المعلومات وانعكاساتها على قانون العقوبات . مطابع الهيئة المصرية العامة للكتاب، مصر، ٢٠٠٣ ، ص ١٩.

٣٣ د. محمد سامي الشواء . المرجع السابق . ص١٩.

٣٤ شمس الدين إبراهيم أحمد . وسائل مواجهة الاعتداءات على الحياة العربية . القاهرة .٢٠٠٥ . ص١ . ص١٠٠.

بتاريخ ١٥/ ٩/ ٢٠١٤ وذلك في الفقرة العاشرة من المادة الأولى من الباب الأول الذي خصصه للتعاريف في تطبيق أحكامه . بأنها: (أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون).[٣٥]

وبذلك لم يترك المشرع القطري تعريف الجريمة الإلكترونية للاجتهادات الفقهية بل نص عليه صراحة منعاً لتلك الاجتهادات التي قد تتوسع في تعريفها أو تضيقه حسب رؤية الفقيه الذي يتناوله بالتعريف.

وهذا ما ورد أيضاً في النظام السعودي لمكافحة جرائم المعلوماتية والذي لم يترك تعريف الجريمة المعلوماتية كما سماها المشرع السعودي للاجتهادات الفقهية بل نص على تعريفها صراحة في الفقرة الثامنة من المادة الأولى من النظام الصادر بالمرسوم الملكي رقم: م/ ١٧ بتاريخ: ٨ / ٣ / ١٤٢٨ هـ والتي عرفها بأنها: (أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام).[٣٦] ويتضح كما جاء في التعريف الذي أورده المشرع السعودي أن الجريمة الإلكترونية هي كل فعل ضار يأتيه الفرد أو الجماعة عبر استعماله الأجهزة الإلكترونية، ويكون لهذا الفعل أثر ضار على غيره من الأفراد [٣٧].

بالبحث في تشريعات كل من سلطنة عمان ودولة الإمارات العربية المتحدة ومملكة البحرين نجد أن المشرع العماني أصدر قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم ٢٠١١/١٢ وقد كان خالياً من النص على تعريف مصطلح الجريمة الالكترونية مكتفياً بتسمية الافعال التي أعتبرها مجرمة ووضع لها العقوبات التي يراها مناسبة لها وذلك في المواد من (٣ إلى ٢٩) من ذات القانون.

أما المشرع الإماراتي فقد أصدر القانون الاتحادي رقم ٢٠٠٦/٢ الخاص بمكافحة جرائم تقنية المعلومات ولم يتطرق إلى تعريف محدد للجريمة الالكترونية وقد ألغي هذا القانون بموجب المرسوم الاتحادي رقم ٢٠١٢/٥ في شأن مكافحة جرائم تقنية المعلومات والذي لم يورد أيضاً تعريفاً للجريمة الالكترونية أو جريمة تقنية المعلومات كما سماها المشرع الإماراتي [٣٨]. وبذلك

---

٣٥ نص الفقرة العاشرة من المادة رقم (١) من القانون القطري رقم ١٤ لسنة ٢٠١٤ م .

٣٦ نص الفقرة الثامنة من المادة رقم (١) من نظام مكافحة جرائم المعلوماتية السعودي .

٣٧ http://droituni.blogspot.com/2013/11 تم النشر قبل 25th November 2013 ـ ٢٠١٥/١/٣ الوقت ٩٥٧.

٣٨ القانون الإماراتي الاتحادي رقم ٢٠١٢/٥ http://www.aecert.ae/laws-ar.php ٢٠١٤/١٢/٢١ الوقت ١٦٤٠.

فأن المشرع الإماراتيساير المشرع العماني إذ لم ينص على تعريف مصطلح الجريمة المعلوماتية وحدد الأفعال التي اعتبرها جرائم إلكترونية في المواد من (٢ إلى ٤٤) من ذات القانون، كما أن التشريع البحريني سلك اتجاه القانونين العماني والإماراتي ولكنه نص على تجريم الأفعال التي تعد جريمة معلوماتية في القانون رقم ٢٠١٤/٦٠ الصادر في ٢٠١٤/٩/٣٠ بشأن جرائم تقنية المعلومات [٣٩]، وعَّرف الأفعال المكونة للجرائم الإلكترونية في المواد من (٢ إلى ١٠)، والمواد من (١٩ إلى ٢١) من ذات القانون.

أما التشريع الكويتي لم نعثر على ما يشير إلى صدور قانون في شأن الجريمة الالكترونية حتى الآن.

ثالثاً: تعريف الجريمة الالكترونية في اتفاقية مجلس أوربا للجريمة الإلكترونية لعام ٢٠٠١:

تم التوقيع على هذه الاتفاقية في ٢٣ نوفمبر ٢٠٠١ في بودابست وتضم في عضويتها ٤٥ دولة أوربية و١٧ دولة من خارج أوربا حتى تاريخ ٢٠١٤/١٠/٥، وعرفت الاتفاقية جرائم الحاسب الآلي في الفصل الثاني بأنها الجرائم ضد السرية والنزاهة وتوافر البيانات وأنظمة الحاسب الآلي في المواد من ٢ إلى ١٢ حيث تم بالترتيب تعريف الدخول غير المشروع، الاعتراض غير القانوني، التدخل في البيانات، التدخل في النظام، إساءة استخدام أجهزة. ثانياً: الجرائم ذات الصلة بالحاسوب: الجرائم المتعلقة بالتزوير، والجرائم المتعلقة بالغش، ثالثاً: الجرائم المتعلقة بالمحتوى: الجرائم المتعلقة بالمواد الإباحية عن الأطفال. رابعاً: الجرائم المتعلقة بانتهاك حقوق الطبع والحقوق المجاورة: الجرائم المتعلقة بالتعدي على حقوق المؤلف والحقوق المجاورة، خامساً: المسؤولية الإضافية: المحاولة والعون والتحريض والمسؤولية المؤسسية في المادة (١٢).

الفرع الثاني

تطور الجريمة الالكترونية

من المعلوم أن هناك صعوبة في تحديد بداية معينة لنشوء الجرائم الإلكترونية ، حيث أن الحواسيب الإلكترونية كانت موجودة منذ فترة بعيدة ، ولكن تختلف عما هي عليه الحواسيب الحالية سواء من حيث الشكل أو السرعة والدقة والتطور الحالي الذي يعتبر نتاج لتطور كبير عبر سنين عديدة.

٣٩ القانون رقم ٢٠١٤/٦٠ الصادر في٣٠/ سبتمبر /٢٠١٤ www.legalaffairs.govptth//:.٢٠١٤/١٢/٢١ الساعة ١٨٠٠ .

إلا أن البعض يرجع حدوث أول جريمة متصلة بالحاسوب إلى عام ١٨٠١م ، عندما أقدم صاحب مصنع للنسيج في فرنسا ويدعى جوزيف جاكوارد Joseph Jacquardعلى تصميم لوحة إلكترونية وكانت أول نموذج للوحة الحاسوب الحالي، لتقوم هذه اللوحة بتكرار مجموعة من الخطوات المستخدمة لحياكة أنواع من المنسوجات، الأمر الذي أثار مخاوف بعض العاملين في المصنع من تأثير تللك اللوحة على وظائفهم مما دفعهم إلى تخريب تلك اللوحة.

بينما يرجع البعض الآخر البداية الحقيقية لظاهرة الجرائم الالكترونية الى عام ١٩٥٨م حينما بدأ معهد ستانفورد الدولي للأبحاث في الولايات المتحدة الامريكية رصد حالات ما سمي في ذلك الحين بإساءة استخدام الحاسوب، بصورة منظمة.

وخلال التسعينيات من القرن العشرين، ومع انتشار الحواسيب والاعتماد عليها في شتى مجال الحياة والأعمال اليومية الخاصة والعامة، بدأت الجريمة الإلكترونية في النمو والبروز أكثر فأكثر، حيث سجل ظهور عدة حالات للجريمة ذات صلة بالحواسيب، كان من أبرزها جريمة سرقة بنك مينيسوتا الأمريكي عام ١٩٦٦م، والتي اعتبرت أول سرقة إلكترونية تقع على بنك[٤٠]. وبعد ذلك توالت بعض المقالات الصحفية في الظهور متناولة بعض الحالات التي أطلق عليها آنذاك جرائم الحاسوب Computer Crime أو الجرائم ذات الصلة بالحاسوب[٤١] Computer-related Crime

ورغم استمرار تطور ظاهرة الجريمة الإلكترونية خلال حقبة السبعينيات، إلا أن الحالات التي سجلت في تلك الفترة الزمنية كانت قليلة، وقد تعود اسباب تلك القلة إلى كون مكمن الخطر كان داخليًا، ويكاد أن يكون خطرا ينحصر بين العاملين على الأنظمة الحاسوبية نفسها حيث كانوا هم فقط من يستطع الوصول إلى تلك الأنظمة بصورة مباشره ولم يكن هناك اتصال بتلك الأنظمة من العالم الخارجي، كما أن سبب قلتها ايضاً يعود إلى عدم الابلاغ عن الكثير من تلك الجرائم لكون الشركات والوكالات كانت تحرص على عدم اهتزاز الثقة بها وبأنظمتها الحديثة ،[٤٢]وأعقبت تلك الحقبة الزمنية إجراء دراسات ومقالات صحفية بشأن

٤٠ محمد بن نصير محمد السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت . دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية: رسالة مقدمة الى كلية الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية كلية الدراسات العليا، ص ١٢ ـ http://www.creativity.ps ٢٠١٤/١٢/٢٧ الوقت ١٦٠٠.

٤١ محمد بن نصير محمد السرحاني . المرجع السابق . ص١٢. http://www.creativity.ps/ ٢٠١٤/١٢/٢٧ الوقت ١٦٠٠ .

٤٢ د. حسين بن سعيد الغافري . جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الانترنت ـ http://hussain-alghafri.blogspot.com/2011/07/blog-post-9603.html 21/12/2014 الساعة ١٨٥٣ .

الجريمة الإلكترونية من قبل كثير من الباحثين الصحفيين.

وفي السبعينيات أيضاً شهد العالم بداية لظهور بعض التشريعات والقوانين التي تجرم بعض الممارسات ذات الصلة بإساءة استخدام الحاسوب وقرّرت لها عقوبات محددة كما حصل في السويد والتي اعُتبرت بذلك أول دولة يصدر فيها قانون يجرم بعض الأفعال والممارسات المرتبطة بالحواسيب[٤٣].

أما في عقد الثمانينيات فقد حدث تغيراً ملحوظاً في التعامل مع ظاهرة الجريمة الإلكترونية وذلك من جانب الباحثين والعامة على السواء بسبب ارتفاع مؤشر عدد القضايا ذات الصلة بإساءة استخدام الحاسوب ولا سيما بعد اهتمام الصحافة وإبرازها لتلك القضايا حيث أصبح بعضها يؤرق المجتمع الدولي كقضايا الاختراق وقرصنة البرمجيات والتلاعب في أنظمة النقد الإلكتروني وانتشار العديد من أنواع الفيروسات[٤٤]. كما شهد ذلك العهد الانطلاقة الأولى للقوانين والتشريعات الخاصة بحماية البرامج الحاسوبية والتي أطلق عليها قوانين حماية الملكية الفكرية واعتبرت من القوانين الاكثر وضوحا ونضجاً.

وكذلك في تلك الفترة الزمنية ظهر الاهتمام العربي بظاهرة الجريمة الإلكترونية وتمثل ذلك في صدور العديد من الدراسات العلمية والمؤلفات العربية ذات الشأن بالجريمة الإلكترونية وعقد الندوات المختلفة ذات الصلة بذلك حيث عقدت في ١٩٨٦م ندوة أمن المعلومات في الحاسبات الآلية والتي تبناها مركز المعلومات الوطني التابع لوزارة الداخلية السعودية [٤٥].

وشهدت التسعينيات والسنوات الأولى من القرن الحادي والعشرين تحولات في مجال الجريمة الإلكترونية حيث ارتبط ذلك بتحول شبكة الإنترنت في ذلك الوقت من شبكة أكاديمية إلى شبكة تعنى بخدمة المجالات التجارية والفردية حيث بلغ مستخدميها في عام ١٩٩٦ ما يقارب ٤٠ مليون مستخدم ، وفي عام ٢٠١٤ تجاوز عدد المستخدمين أكثر من ثلاثة مليار مستخدم الامر الذي أدى إلى خلق عبء كبير على المختصين بمكافحة الجريمة الإلكترونية ولذلك وُجد مفهوم جديد عرفها (بالجرائم العابرة)، حيث يستطيع المجرمون تنفيذ مخططاتهم الاجرامية في

٤٣ عبدالله حسين آل حجراف القحطاني ـ تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية ـ دراسة تطبيقية في هيئة التحقيق والادعاء العام بمدينة الرياض، رسالة ماجستير، الرياض، ١٤٣٥ـ٢٠١٤م، ص٣٠.
repository.nauss.edu.sa٣٠ptth://٢٠١٤/١٢/ الوقت ١٧٠٠

٤٤ عبدالله حسين آل حجراف القحطاني، المرجع السابق، ص٣٠. repository.nauss.edu.saptth:// ٢٠١٤/١٢/٣٠ الوقت١٧٣٠

٤٥ عبدالله حسين آل حجراف القحطاني، المرجع السابق، ص٣١. repository.nauss.edu.saptth:// ٢٠١٤/١٢/٣٠ الوقت١٧٣٠

دول متعددة دون الاكتراث بأية حدود دولية [٤٦]. وفيما يتعلق بالجهود الدولية لمواجهة الجريمة الإلكترونية، سيتم تناولها بالتفصيل المناسب في المبحث الرابع.

المطلب الثاني
أسباب الجريمة الالكترونية وآثارها

لكي نتعرف على أسباب الجريمة الالكترونية وآثارها نقسم هذا المطلب إلى فرعين حيث سنخصص الفرع الاول لأسباب الجريمة الالكترونية والفرع الثاني سنبين من خلاله الآثار التي تنتج عن الجريمة الالكترونية.

الفرع الأول
أسباب الجريمة الالكترونية

لا شك أن مرتكبي الجريمة الإلكترونية يختلفون عن مرتكبي الجريمة التقليدية ، ويرجع ذلك لاختلاف الاشخاص من حيث السن والجنس والمستوى التعليمي وغير ذلك من المؤثرات الخارجية، كما أن الأسباب أو الدوافع التي تدفعهم لارتكاب الجريمة هي أيضاً تختلف، حيث أنها العوامل المحركة للإرادة التي توجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام وكسب المال، فهي القوة النفسية التي تدفع الإرادة لارتكاب الجريمة ابتغاء تحقيق غاية معينة ، ولذلك فإن الجريمة الالكترونية تختلف عن الجريمة التقليدية ، وتبعاً لذلك فأن الأسباب والدوافع التي تدفع الجناة لارتكاب الفعل غير المشروع لها تختلف عن الاسباب والعوامل التي تدفع الجناة لارتكاب الفعل غير المشروع للجريمة التقليدية[٤٧]. ويأتي في مقدمة أسباب ودوافع الجريمة الإلكترونية، ثمة أسباب ودوافع تتمثل في الرغبة أو الولع بجمع المعلومات التي قد تكون محفوظة في أجهزة الحاسب الآلي أو منقولة عبر الشبكة العالمية للمعلومات كما قد تكون الأسباب والدوافع الرغبة في الاضرار بالغير من جهات معينة وأشخاص وكذلك الرغبة في الربح والكسب الذي قد يدفع إلى التعدي على الحواسيب ونظم المعلومات إضافة إلى الدوافع الشخصية

---

٤٦ عبدالله حسين آل حجراف القحطاني: المرجع السابق، ص ٣٢ ـ repository.nauss.edu.saptth:// ٢٠١٤/١٢/٣١ الوقت ٧٠٠

٤٧ د. حسين بن سعيد الغافري. جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الانترنت http://hussain-alghafri.blogspot.com/2011/07/blog-post-9603.html ٢٠١٤/١٢/٢١ الساعة ١٨٥٣ .

للجاني لإبراز الذات التي قد تكون سبباً في ارتكاب الجريمة المعلوماتية[٤٨]. ونذكر بعضاً من تلك الاسباب والدوافع فيما يلي:

١ـ الرغبة في جمع المعلومات وتعلمها.

وأولئك الذين يرتكبون هذه الجرائم يقدمون عليها بغية الحصول على الجديد من المعلومات وقد أشار الأستاذ ليفي في أحد مؤلفاته الخاصة بقرصنة الأنظمة (HACKERS) إلى (أن أخلاقيات هؤلاء القراصنة ترتكز على مبدأين أساسين هما الأول: أن الدخول إلى أنظمة الحاسب الآلي يمكن أن يعلمك كيف يسير العالم ، والثاني أن جمع المعلومات يجب أن يكون غير خاضع للقيود)[٤٩]. ومن وجهة نظر هؤلاء القراصنة فإن جميع المعلومات المفيدة بوجه عام يجب أن تكون غير خاضعة للقيود وبعبارة أخرى أن تتاح حرية نسخها وجعلها تتناسب مع استخدامات الأشخاص. وكثيراً ما نجد أن قراصنة الأنظمة يعلنون أن هدفهم من الوصول للمعلومات ودخولهم للشبكات والحواسيب الالكترونية هو التعلم فقط. فهم يتعاونون في البحث على شكل جماعات ويتقاسمون المعلومات والخبرات التي يحصلون عليها ويستفيدون منها في أنشطة هادفة ولو بطرق غير مشروعة.[٥٠]

٢ـ الاستيلاء على المعلومات.

الاقدام على ارتكاب هذا الجرم بواسطة تقنية المعلومات بهدف الحصول على المعلومة ذاتها والاستيلاء عليها والتصرف فيها يتمثل ذلك في الحصول على المعلومة المحفوظة في الحاسب الآلي أو المنقولة أو تغييرها أو حذفها أو إلغائها نهائياً من النظام. ويختلف الدافع لهذا التصرف فقد يكون دافع تنافسي أو سببه الابتزاز أو الحصول على مزايا ومكاسب اقتصاديه ، كثيراً ما يكون هدف هذه الجرائم ذو طابع سياسي أو اقتصادي.

٣ـ قهر النظام وإثبات التفوق على تطور وسائل التقنية.

في بعض الأحيان يكون الدافع وراء ارتكاب هذه الجرائم هو قهر النظام وإثبات قدرة الجاني وتفوقه على تعقيدات وتطور وسائل التقنية الحديثة، حيث يمضي كل وقته أمام شاشات أجهزته لكسر الحواجز الامنية للأنظمة الإلكترونية واختراقها ليثبت براعته في القدرة على تحدي

---

٤٨ http://accronline.com/article-detail.aspx?id=7509 . ٢٠١٤/١٢/٢٠ الساعة ٢٠١٤ .

٤٩ د. حسين بن سعيد الغافري . مرجع سابق . ص ٤ـ http://hussain-alghafri.blogspot.com 21/12/2014 الساعة ١٨٥٣.

٥٠ د. حسين بن سعيد الغافري . مرجع سابق . ص ٤. http://hussain-alghafri.blogspot.com 21/12/2014 الساعة ١٨٥٣.

أي تطور جديد في عالم التقنية والتكنولوجيا. ويرتفع مؤشر الزيادة لدى فئات صغار السن من مرتكبي هذه الجرائم .[٥١]

٤ـ إلحاق الأذى بأشخاص أو جهات.

بعض المجرمين الذين يقدمون على ارتكاب الجريمة عبر شبكة المعلومات العالمية وتقنية المعلومات بصورة عامة يتركز الدافع من ورائها على إلحاق الأذى بأشخاص محددين أو جهات معينة ، وغالبا ما تكون تلك الجرائم مباشرة تتمثل في صورة ابتزاز أو تهديد أو تشهير كما حصل في القضية التي تم ضبطها بإمارة دبي بدولة الإمارات العربية المتحدة عندما أقدم الجاني فيها ويلقب «بقرصان صور الفتيات» بالسطو على البريد الإلكتروني لمجموعة من الفتيات بتلك الدولة والاستيلاء غير المشروع على صورهن الشخصية وتعمد نشرها على موقع خاص بشبكة الإنترنت مع مجموعة الصور الإباحية. وكما يمكن أن تكون هذه الجرائم غير مباشرة وتتمثل في الحصول على البيانات والمعلومات الخاصة بتلك الجهات أو الأشخاص لاستخدامها فيما بعد في ارتكاب جرائم مباشرة.[٥٢]

٥ـ تحقيق أرباح ومكاسب مادية.

هناك بعض الجرائم الإلكترونية التي ترتكب يكون الدافع منها تحقيق أرباح ومكاسب مادية كاستخدام شبكة الإنترنت للإعلان عن صفقات تجارية غير مشروعة كصفقات المخدرات والاتجار بالبشر وقد ورد في بحث أعده هشام بشير المستشار الإعلامي للجمعية المصرية لمكافحة جرائم الإنترنت أن عصابات الإجرام المنظم استغلت التكنولوجيا الحديثة في تيسير شئون الاتجار في البشر ويرى الباحث أن الاتجار بالبشر عبر الإنترنت هو تجارة الإلكترونية حيث أن تعريف التجارة الإلكترونية تلك التعاملات التي تتم الكترونيا عبر شبكة المعلومات العالمية (الإنترنت)[٥٣].

---

٥١ http://hussain-alghafri.blogspot.com 21/12/2014 الساعة ٧٥٠ .

٥٢ http://hussain-alghafri.blogspot.com 21/12/2014 الساعة ٨٢٣ .
د. حسين بن سعيد الغافري . مرجع سابق . ص ٤ .

٥٣ http://www.google.comwww.dhd4train.com%2Fdata%2Flearn-with-us%2Fcrim ٢٢/١٢/٢-١٤ الساعة٩٠٤.

٦ـ تهديد الأمني القومي والعسكري.

بعض الجرائم الالكترونية الهدف منها أسباب ودوافع سياسية كتهديد الأمن القومي والعسكري ومن ذلك ظهر ما يعرف بالتجسس الإلكتروني والإرهاب الإلكتروني والحرب المعلوماتية كما هو الحاصل بين الدول المتقدمة إلكترونياً [٥٤].

الفرع الثاني
آثار الجريمة الالكترونية

شهد العالم في الفترة الأخيرة ارتفاعا ملحوظاً في مؤشر عدد الجرائم الإلكترونية صاحبه تطور نوعي في المستوى الحرفي للجناة الذين ارتكبوا تلك الجرائم التي لا تعترف بحدود معينة لبلد معين ، ومع هذه الطبيعة العالمية لهذه الجرائم التي تؤثر على الاقتصاد العالمي فإن ذلك التأثير الناجم عنها يفوق بكثير الآثار الاقتصادية التي تنجم عن الجرائم التقليدية.[٥٥] وأظهرت نتائج دراسة تم نشرها في ٢٠١٣/٠٥/٣٠ أجراها بنك إتش إس بي سي بالاشتراك مع مجموعة الدراسات العالمية نيلسن (أن الجرائم الإلكترونية في دولة الإمارات العربية المتحدة كبدت اقتصاد الدولة خلال عام ٢٠١٢ خسارة بلغت نحو ٤٢٠ مليون دولار)[٥٦]. وأشارت دراسة جديدة نشرت في ٩ يونيو ٢٠١٤ إلى أن جرائم الإنترنت تكلف الاقتصاد العالمي نحو ٤٤٥ مليار دولار كل عام، وأن الأضرار التي لحقت بقطاع الأعمال نتيجة سرقة حقوق الملكية الفكرية تتسبب بخسارة الأفراد لحوالي ١٦٠ مليار دولار[٥٧]. كما ذكر التقرير الصادر عن مركز الدراسات الاستراتيجية والدولية CSIS أن الجريمة الإلكترونية تضر بالتجارة والقدرة على التنافس والابتكار. وهناك دراسة ترعاها شركة البرمجيات الأمنية (مكافي) ، تشير تقديراتها إلى أن الخسائر وصلت إلى٤٥٠ مليار دولار، في حين أن الحد الأقصى لتقديرات الخسائر قد يبلغ ٥٧٥ مليار دولار.[٥٨] كما ذكرت الدراسة أيضاً أنه بلغ إجمالي خسائر الولايات

---

٥٤ http://hussain-alghafri.blogspot.com 21/12/2014 الوقت: ٨٤٠ . د/ حسين بن سعيد الغافري . مرجع سابق . ص ٤ .
http://accronline.com/article-detail.aspx?id=7509 ٢٠١٤/١٢/٢٢الوقت: ٩٤٥

٥٥ http://www.aldaawah.com/?p=7833 ـ الدكتور نبيل صلاح محمد العربي، أستاذ مساعد بكلية الاقتصاد والإدارة – جامعة القصيم دراسة بعنوان ''اقتصاديات الجرائم المعلوماتية ''.

٥٦ تقرير حول المخاوف الأمنية والخصوصية وراء الفجوة الإقليمية في الخدمات المصرفية الإلكترونية . نشر بتاريخ ٢٠١٣/٠٥/٣٠ . المصدر : (دبي – عبير أبو شمالة) ـhttp://www.alkhaleej.a

٥٧ http://aitnews.com/2014/06/09 . ٢٠١٤/١٢/٢٤ . الوقت ١٠٢٣.

٥٨ http://aitnews.com/2014/06/09 . ٢٠١٤/١٢/٢٤ . الوقت ١٠٢٣.

المتحدة والصين واليابان والمانيا ٢٠٠ مليار دولار سنويًا، كما بلغت الخسائر المرتبطة بالبيانات الشخصية كبيانات بطاقات الائتمان، ١٥٠ مليار دولار. وفي بيان لجيم لويس، العامل لدى CSIS ذكر إن الجريمة الإلكترونية تبطئ وتيرة الابتكار العالمي بتقليل معدل العائد للمبدعين والمستثمرين وكما أنها لها آثار خطيرة على العمالة ولا سيما في الدول المتقدمة.[٥٩] وهناك تأثيرات للجريمة الالكترونية على مستوى الفرد الذي قد يتعرض لها والتي تؤثر على الجانب المادي لديه ربما نوجز بعضاً منها فيما يلي:

سرقة الهوية الشخصية- سرقة بطاقة الائتمان الخاصة به- الابتزاز والتهديد- عمليات احتيال- تحويل أو نقل حسابه المصرفي- نقل ملكية الأسهم- زيادة الفواتير بتحويل فواتير المجرم للضحية.[٦٠]

---

٥٩ http://aitnews.com/2014/06/09 ـ ٢٠١٤/١٢/٢٤ . الوقت ١٠٢٣.

٦٠ الكاتبة/ منى شاكر فراج العيسلي: مقال بعنوان تأثير الجريمة الالكترونية على النواحي الاقتصادية.
://www.shatharat.net/vb/showthread.phpptth ٢٠١٤/١٢/٢٤ الوقت ١٧٢٧ .

المبحث الثاني
واقع الجريمة الإلكترونية ووسائل مكافحتها

مقدمة:

نستنتج واقع الجريمة الإلكترونية من المراحل التي مرت بها نشأتها في بداية عقد السبعينات من القرن الماضي ومن التطورات التكنولوجية المتلاحقة في أنظمة تقنية المعلومات والاتصالات والزيادة المتسارعة في استخدام أجهزة الحاسب الآلي والإنترنت في نشاطات أجهزة الدولة والقطاع الخاص والأفراد، حيث وصل عدد مستخدمي الإنترنت إلى أكثر من ثلاثة مليار في ١ يوليو ٢٠١٤ بنسبة ٤٠٪ من عدد سكان العالم، وبناء على ما تقدم ارتفعت معدلات الجريمة الإلكترونية وتضاعف حجم الخسائر وأصبح لابد من إيجاد الحلول لمواجهتها والحد منها.

نتناول موضوعات هذا المبحث في مطلبين كما يلي:

المطلب الأول: حجم الجريمة الإلكترونية ونطاقها.

المطلب الثاني: وسائل مكافحة الجريمة الإلكتروني.

المطلب الأول
حجم الجريمة الإلكترونية ونطاقها

مع تحقق الاندماج الكبير بين الحوسبة والاتصالات وولادة المدلول الشامل لتقنية المعلومات فقد شهدت حقبة سبعينات القرن الماضي الانطلاقة الحقيقية للدراسات والبحوث المتخصصة في مجال تقانة المعلومات، فقد أجريت دراسات مسحية وأبحاث عديدة أهمها:[٦١]

أ- دراسة معهد استانفورد العالمي للأبحاث في الولايات المتحدة ١٩٧٣ التي رصدت (١٦٠) حالة لإساءة استخدام أجهزة تقانة المعلومات منذ عام ١٩٥٨ وشملت الدراسة استبيان المعهد عام ١٩٦٩ الموجه إلى ٧٢ مدعياً عاماً حيث أشار ٤٠ منهم بوصول ١٩٠ جريمة إلى علمهم وتمت ادانة ٣٣٧ متهم.

ب- دراسة مكتب المحاسبة العامة (الولايات المتحدة الأمريكية ١٩٧٦) التي رصدت ٧٤ جريمة.

---

٦١ محمود العطا: دور التشريعات والإجراءات الأمنية في التصدي للإجرام المعلوماتي، رسالة دكتوراه (بحث غير منشور)، جامعة الرباط الوطني، الخرطوم، السودان ٢٠٠٧، ص٣٠

ج- دراسة معهد الاجرام وقانون العقوبات الاقتصادي في المانيا عام ١٩٧٧، والتي اعتمدت على تقرير تجميعي نشره مستشار للأمن الالماني عام ١٩٧٣ حيث تضمنت الدراسة عدد ٣١ جريمة ارتكبت بواسطة أجهزة تقانة المعلومات.

د- دراسة معهد كولفيلد للتقنية Coalfield بأستراليا (٧٥- ١٩٨٥) حيث قام القسم المختص بأبحاث إساءة استخدام الحاسوب التابع للمعهد بهذه الدراسة في الفترة من ١٩٧٥- ١٩٨٥ ورصدت الدراسة ١٥٠ حالة.

هـ- دراسة المكتب المركزي للشرطة اليابانية (طوكيو ١٩٧٢) والتي رصدت ٣٦ حالة.

و- كما ظهرت العديد من الدراسات المتخصصة والمتعمقة حول جرائم أجهزة تقانة المعلومات وكان من أشهرها جرائم الكمبيوتر للباحث Bigots Bacau عام ١٩٧٨، وكذلك دراسة الاجرام بواسطة الكمبيوتر للباحث الأمريكي D.B.Parker عام ١٩٧٨.

كان اتجاه الدراسات إلى البحث في الأبعاد والمضامين القانونية لظاهرة الاجرام الموجه إلى المعلومات، بالإضافة للاهتمام بالبيانات الشخصية والأنشطة المستهدفة للاعتداء على الحياة الخاصة، حيث توج هذا الاهتمام بولادة حزمة من التشريعات الخاصة بحماية الخصوصية المعلوماتية ، بإيراد بعض الدول لهذه الحماية في دساتيرها كما هو الحال في الدستور الاسباني ١٩٧٨ والدستور البرتغالي ١٩٧٦.(٦٢)

في العام ١٩٩٥ أنشئ في الولايات المتحدة الامريكية معهد الفضاء السيبرانيCyber Law Institute في جامعة جورج تاون حيث يوجد به عدد كبير من المتخصصين في هذا المجال يعملون على تحديد كيفية التعامل مع مشكلات الفضاء الإلكتروني.(٦٣)

تلاحق إصدار القوانين الخاصة بتنظيم استخدام أجهزة تقنية المعلومات في معالجة البيانات ومواجهة الاعتداء عليها، وفي هذا الإطار نشأت مفاهيم ونظريات جديدة للمعاملات المتصلة بالشبكة العالمية للمعلومات، منها على سبيل المثال:

أ- تشريعات الملكية الفكرية التي تضم العلامات التجارية والملكية الفنية والأدبية للمصنفات الرقمية وحماية براءات الاختراع على المنتجات الرقمية.

---

٦٢ يونس عرب: جرائم الكمبيوتر والإنترنت، منشورات اتحاد المصارف العربية، الاردن، ٢٠٠٢، ص٢٧.

٦٣ يونس عرب: النظام القانوني للخصوصية الرقمية، منشورات اتحاد المصارف العربية، الاردن، ٢٠٠٢، ص٣٥.

ب- تشريعات جرائم الكمبيوتر ومن ثم تطورها لتشمل جرائم شبكة المعلومات العالمية ضمن مفهوم أشمل هو أمن المعلومات.

ج- تشريعات الخصوصية أو قواعد حماية تجميع ومعالجة وتخزين وتبادل البيانات الشخصية.

د- تشريعات المحتوى الضار الخاصة بحماية الشبكة من الدخول غير المشروع بما في ذلك الاقتحام الفيروسي.

هـ- تشريعات التجارة الإلكترونية التي تشمل التسوق الإلكتروني والتعاقدات الإلكترونية والتوقيع الإلكتروني.

و- تشريعات الاستثمار والتجارة والجمارك والاتصالات والضرائب والأنظمة الحكومية المرتبطة بالمشروعات التقنية ذات الصلة بتقانة المعلومات.

ز- التشريعات المالية والمصرفية ذات الصلة بالمال الإلكتروني وتقنيات الخدمات المصرفية في بيئة الشبكة العالمية للمعلومات.

يتضح من كثافة هذه التشريعات أن هناك مجالاً خصبا للتعاملات قد يتعرض للاعتداءات، وقد بدأ الفقه وتبعه التشريع والقضاء، في محاولات لتنظيم تلك المسائل لمواكبة التطورات في مجال المعلوماتية وقد بدأت ملامح التنظيم القانوني الدولي والمقارن لتقنية المعلومات في الظهور في إطار الحماية القانونية للمعلومات والاداء الرقمي.

حجم استخدام (شبكة الانترنت) عالمياً:

من خلال الطرح السابق يمكننا التأكيد بأن الجريمة الإلكترونية ترتبط ارتباطاً مباشراً بشبكة المعلومات العالمية الانترنت، وقد جرى تعريف مستخدم الانترنت بأنه كل شخص يمكنه الوصول للإنترنت في المنزل باستخدام الحاسب الآلي أو جهاز الهاتف الجوال.

وفقاً لموقع Internet Live Stats. com فإن ٤٠٪ من سكان العالم يستخدمون الانترنت[٦٤]، وقد بلغ عدد المستخدمين للإنترنت وفقا للموقع ٢٩٢٥٢٤٩٣٥٥ مستخدم بنسبة نمو تعادل ٧,٩٪ بينما بلغ نمو السكان ١,١٤٪ مما يؤكد زيادة نسبة معدلات استخدام الإنترنت. ويترتب على زيادة استخدام الإنترنت منطقياً زيادة في نسبة المخالفات التي ترتكب من جراء هذا الاستخدام والتي قد تصل حد الفعل المجرم.

٦٤ إحصائية استخرجت في سبتمبر ٢٠١٤ Inerrant Live Stat - www.Internet Live Stats- com

ووفقاً لإحصائيات الموسوعة الحرة[٦٥] الخاصة بقائمة الدول المستخدمة للإنترنت، فقد ضمت القائمة عدد ٢١٢ دولة تستخدم الإنترنت بمجموع سكان يعادل ٤٠٪ من سكان العالم يستخدمون الإنترنت بعدد مستخدمين بلغ ٢٩٢٥٢٤٩٣٥٥ مستخدم وهذا ما أكدته إحصائية لايف انترنت في ذات الفترة التاريخية.[٦٦]

في عام ٢٠١٢تصدرت الصين قائمة الدول الأكثر استخداماً بنسبة السكان بعدد مستخدمين بلغ ٥٦٨١٩٢٠٦٦ فرداً من السكان، ولكن برغم ذلك كان ترتيبها رقم ١٠٢ بالنسبة للاستخدام العالمي للإنترنت، بينما تصدرت مصر قائمة الدول العربية في عدد السكان المستخدمين للإنترنت حيث بلغ مجموعهم ٣٦٨٨١٣٧٦، وكان ترتيبها رقم ٩٩ بالنسبة للاستخدام العالمي للإنترنت وقد تصدرت المملكة العربية السعودية قائمة الدول الخليجية في عدد السكان المستخدمين للإنترنت حيث بلغ مجموعهم ١٤٣٢٨٦٣٢، وكان ترتيبها رقم ٧٩ بالنسبة للاستخدام العالمي.[٦٧]

باستنباط نسبة السكان المستخدمين للإنترنت في الدول أعلاه نجد أن النسبة في الصين تبلغ ٤٢,٣٪ وبلغت النسبة في مصر ٤٤,١٪ بينما بلغت النسبة في المملكة العربية السعودية ٥٤٪.

ووفقاً لموقع www.Internet Live Stats-com يلاحظ نسبة النمو المضطردة في استخدام الإنترنت بواسطة السكان في العالم، حيث بلغت نسبة زيادة المستخدمين في العام ٢٠١٤[٦٨] في بعض الدول كالتالي:

١- الصين نسبة الزيادة في الاستخدام السكاني بلغت ٤٪.
٢- أفغانستان نسبة الزيادة في الاستخدام السكاني بلغت ١٠٪.
٣- أثيوبيا (نموذج أفريقي) نسبة الزيادة في الاستخدام السكاني بلغت ١٦٪.
٤- السلفادور نسبة الزيادة في الاستخدام السكاني بلغت ٧٪.
٥- فرنسا (نموذج أوربي) نسبة الزيادة في الاستخدام السكاني بلغت ٣٪.

---

٦٥ إحصائيات لايف انترنت سبتمبر ٢٠١٤. Inerrant Live Stat - www.Internet Live Stats- com

٦٦ الموسوعة الحرة سبتمبر ٢٠١٤. Inerrant Live Stat - www.Internet Live Stats- com

٦٧ الموسوعة الحرة سبتمبر ٢٠١٤. Inerrant Live Stat - www.Internet Live Stats- com

٦٨ إحصائية يوليو ٢٠١٤. Inerrant Live Stat - www.Internet Live Stats- com

تم تقديم تقديرات مستخدمي الإنترنت بواسطة مؤسسة world meters RTS algorithm التي قامت بمعالجة بيانات مفصلة من خلال تحليلات إحصائية بعد أن تم جمعها من المصادر التالية:[٦٩]

أ- تقرير الاتحاد الدولي للاتصالات I.T.U.

ب- شعبة الأمم المتحدة للسكان التقرير نصف السنوي للعام ٢٠١٤.

ج- تقرير جمعية الانترنت الجوال في الهند IAMAI.

د- تقرير البنك الدولي النصف السنوي للعام ٢٠١٤.

هـ- تقرير وكالة المخابرات المركزية الأمريكية.

نخلص إلى أن زيادة نسبة الاستخدام للإنترنت بالنسبة للدول أو السكان بنسب مضطردة يترتب عليه زيادة احتمالات الاستعمال غير الرشيد الذي قد يصل إلى حد الفعل المجرم، لاسيما وأن الظروف مواتية لزيادة استخدام الانترنت والوصول إلى الانترنت عبر وسائط أجهزة تقنية المعلومات التي أصبحت في متناول الجميع، وتتعزز هذه الفرص مع التطور الكبير في أجيال الهواتف النقالة الذكية، بالإضافة إلى المنافسة في سوق الاتصالات بين المشغلين مما يزيد اهتمام الناس بهذه الخدمات.

الملحق رقم (٣) يمثل قائمة بالدول المستخدمة للإنترنت على مستوى العالم عام ٢٠١٤، حيث تصدرت الصين القائمة بعدد السكان المستخدمين بينما جاء ترتيبها رقم ١٠٢ على مستوى العالم، بينما تصدرت جزر الفوكلاند وايسلندا على التوالي قائمة الدول التي يستخدم مواطنوها الإنترنت بنسبة تتجاوز ٩٦٪ من السكان يليهم في الترتيب مجموعة الدول الإسكندنافية (النرويج والسويد والدنمارك) التي يستخدم مواطنوها شبكة الإنترنت بنسبة تزيد عن ٩٥٪.

إشكال وأنماط الجريمة الإلكترونية في مجتمع دول مجلس التعاون الخليجي:

يلاحظ أن معدلات الجرائم الإلكترونية في ارتفاع مستمر عالمياً، ووتيرة أسرع في المجتمعات الخليجية، وذلك ناتج عن:

أ- التحسن المستمر في سرعات الاتصال بالإنترنت.

ب- انتشار أجهزة الحاسوب الشخصي Laptop وأجهزة الاتصال التلفوني النقالة الذكية.

---

٦٩ Inerrant Live Stat - www.Internet Live Stats- com مستخرجة بتاريخ ٨ يناير ٢٠١٥.

ج- زيادة استخدام البرمجيات سواء في الشركات الكبرى وأنشطة الأعمال، أو تطبيقات الوسائط الاجتماعية.

د- تنفيذ برامج وخدمات الحكومة الإلكترونية والأنشطة المصرفية عبر الإنترنت.

ووفقاً للدراسة المسحية التي قدمتها شركة كاسبر سكاي المتخصصة في أمن المعلومات حول مخاطر أمن المعلومات في الشركات العالمية[٧٠]، فإن الهجمات الإلكترونية هي السبب الرئيسي في تسرب البيانات السرية من المنشآت، حيث ذكرت الدراسة أن ١٨٪ من المنشآت الخليجية تعاني من تسرب بياناتها بعد تعرضها لمثل هذا النوع من الهجمات، واشارت الدراسة بأن التهديدات الإلكترونية في تزايد مستمر عالمياً، وتحديداً هجمات التصيد Fishing Attack هي أكثر التهديدات التي تواجه الشركات والأعمال بصورة متكررة، والهدف الأساسي لهذه الهجمات هي تصيد البيانات للحصول على الرقم السري وتفاصيل الدخول وبيانات البطاقة الائتمانية وغيرها الخاصة بالشركات والمصارف والمؤسسات الرسمية وغيرها.

في العام ٢٠١٠ ذكر تقرير Norton Symantec المتخصص في رصد الجريمة الإلكترونية، أن خسائر الجرائم المعلوماتية في العالم تقدر بحوالي ١٤٤ مليار دولار، وذكر التقرير اللاحق في العام ٢٠١١ إن عدد البالغين الذين تعرضوا لهجمات وتهديدات ومخاطر عن طريق الانترنت يقدر عددهم بـ ٤٣٢ مليون شخص حول العالم، وذكر ذات التقرير أن خسائر الانترنت والجرائم المعلوماتية وصلت إلى ٣٨٨ مليار دولار حول العالم، والذي تجاوز قيمة الخسائر للجرائم التقليدية الأخرى كتجارة المخدرات التي بلغت ٢٨٠ دولار.

وكشف تقرير نورتن سيماتتيك في العام ٢٠١٢ أن خسائر دول مجلس التعاون الخليجي من جراء جرائم المعلوماتية بلغت ٨٥٠ مليون دولار، بينما تجاوزت الخسائر لذات دول الخليج في العام ٢٠١٣ مبلغ ٩٠٠ مليون دولار، وكشف التقرير نفسه أن خسائر الجرائم المعلوماتية في المملكة العربية السعودية بلغت ٥٢٧ مليون دولار.[٧١]

هذه الأرقام والإحصائيات تنبئ بمخاطر كبيرة، وتعطى مؤشرات، وتلفت أنظار صناع القرار للتحرك لمواجهة هذه الجرائم وخطورتها، كما أن الهجمات الإلكترونية التي تعرضت لها كل من المملكة العربية السعودية ودولة قطر في الأعوام ٢٠١٢/ ٢٠١٣ على التوالي باستهداف

---

٧٠ Cybercrime. Kaspersky.com إبريل ٢٠١٤- موقع: AR- Wikipedia- org. Indie

٧١ Norton Symantec.2013 Norton Report

شركة أرامكو السعودية للنفط وشركة رأس غاز القطرية، وفي عام ٢٠١٣ اطلقت هجمات على مواقع إلكترونية سعودية حكومية أدت إلى تعطيل بعض المرافق مؤقتاً منها وزارة الداخلية وهذه الهجمات تمثل جرس إنذار وتنبيه للحكومات في دول مجلس التعاون الخليجي.[٧٢]

وفي تقرير نورتن سيمانتيك Norton Symantec للعام ٢٠١٣ فقد وردت كلاً من المملكة العربية السعودية ، ودولة الإمارات العربية المتحدة من دول مجلس التعاون الخليجي، ضمن الـ ٢٤ دولة الأولى في العالم التي تزيد فيها التهديدات المقلقة بتسرب البيانات.[٧٣]

وفي دراسة أخرى لكاسبر سكاي، إشارة إلى أن دولة الإمارات العربية المتحدة أحتلت طليعة دول الشرق الأوسط (وليس الخليج فحسب) الأكثر استهدافاً وعرضة للجرائم المالية الإلكترونية بنسبة تقدر بـ ٣٨,٨٪ تليها المملكة العربية السعودية بنسبة تقدر بـ ٢٩,٣٪، تليهم خليجياً دولة قطر بنسبة ٩,٦٤٪ ، والكويت بنسبة ٦,٩٢٪ ، وصنف التقرير المملكة العربية السعودية ضمن التصنيف (عالي المخاطر) في مجال التعرض للتهديدات والمخاطر المتعلقة بالاتصالات وتقنية المعلومات والشبكات المعلوماتية.[٧٤]

تتيح إحصائيات الجريمة الإلكترونية، واكتشافاتها ومكافحتها إمكانية تحليل الواقع، وعمل مقارنات ومقاربات محلية وإقليمية ودولية، ومن ثم تحديد نقاط الضعف والقوة، وكذلك يمكن تحديد الفرص، كما تتيح أيضاً إبراز التهديدات وتحديد ابرز الفجوات، سواء كانت أمنية أو تشريعية وغير ذلك، مع التركيز على تحديد التهديدات والمخاطر التي تواجه المجتمع الخليجي بتطوره المتسارع نحو التحول إلى مجتمع المعرفة، واقتصاد المعرفة، المعتمد على تطبيقات تقنية الاتصالات والمعلومات.

ووفقاً لمجلة ميد (www.Meed.com) فإن الشركات الخليجية التي تتعامل بالأدوات المالية ستبقى هدفاً لعصابات الجريمة الإلكترونية المنظمة وذلك بناء على تقارير صادرة عن جمعية التجارة الإلكترونية المتخصصة في رصد ومتابعة الجرائم الإلكترونية ومراقبتها والتحذير من مخاطرها.[٧٥] لاسيما وأنه وفقاً للمجلة فقد شن القراصنة من خارج السعودية في مايو ٢٠١٣ هجمات منسقة على مواقع الكترونية حكومية مما أدى الى تعطل موقع وزارة الداخلية بصورة مؤقتة.

---

٧٢ www.reuters.com.article/17May 2013 - وكالة رويتر.

٧٣ Norton Symantec 2014 / تقرير العام ٢٠١٣.

٧٤ AR- Wikipedia- org. Indie- Cybercrime. Kasper. com مستخرجة بتاريخ ٢٠١٤/٩/٢٣.

٧٥ www.Meed.com/sector/Markets/ commodities/ 28 May 2014

من التقارير أعلاه يلاحظ تنامي التهديدات الأمنية الالكترونية على منطقة الخليج حيث بلغت نسبة زيادة التهديدات في العام ٢٠١٣ بلغت ٥٠٪ مقارنة بالعام ٢٠١٢ ويتوقع زيادة مماثلة في العام ٢٠١٤ وتأكيداً لذلك ما ورد عن شركة مكافي (McAfee) المتخصصة في الحلول الأمنية الإلكترونية ومكافحة الفيروسات أن العام ٢٠١٣ شهد تدفقاً كبيراً للهجمات الإلكترونية على الإمارات العربية والمملكة السعودية من مصادر قرصنة اسرائيلية.[٧٦]

أظهر تقرير مختص بجرائم الإنترنت[٧٧] أن الهجمات الإلكترونية في عالم الأعمال في الإمارات المتحدة تسببت في خسائر فاقت ٤٢٢ مليون دولار في العام ٢٠١٢ وأن عدد الأشخاص ضحايا جرائم الكترونية قد بلغ ١,٥ مليون شخص مع ملاحظة أن معظم الشركات تكتمت على ما يحدث عليها من اختراقات وقد بلغت تكلفة الهجمات الإلكترونية على الأفراد السعوديين ٥٢٧ مليون دولار في العام ٢٠١٣.

أكدت دراسة شركة الخليج للحاسبات الآلية G.BM في يونيو ٢٠١٣[٧٨] على ما ورد في التقارير السالف ذكرها، حيث ذكرت أن خبراء تكنولوجيا المعلومات في دول مجلس التعاون الخليجي يؤكدون أن منطقة الخليج تشكل هدفاً رئيسيا للجرائم الإلكترونية كما ذكرت الدراسة أن زيادة شبكات التواصل الاجتماعي يصاحبه ازدياد في مخاطر الأمن الإلكتروني.

في ابريل ٢٠١٤ كشفت Kasper Skylab عن خريطة للعالم يتم بها تتبع التهديدات الإلكترونية المختلفة وأعدادها[٧٩] وتوضح من خلالها أكثر الدول استهدافاً من جراء تلك التهديدات وقد كانت المحصلة كالتالي:

أ- احتلت المملكة العربية السعودية المرتبة الأولى عربيا والمرتبة العشرون عالمياً من حيث التهديدات.

ب- جاءت دولة الإمارات العربية في المرتبة الثانية عربياً والمرتبة الثانية والعشرون عالميا من حيث التهديدات.

هـ- وكانت سلطنة عمان في المرتبة الثالثة عربياً والمرتبة السادسة والخمسون عالمياً.

---

٧٦ www.Alarabiya .net/ar/techonlgy. 31 Jan 2013 موقع العربية

٧٧ cost of cyber crime study repent. H.P Enterprise security. www.Jlegt- com. 28 Jan 2014

٧٨ www.artnews.com/26 June 2013

٧٩ Cyber Threat Map. 28 May 2014 AR- Wikipedia- org. Indie-

بتاريخ ٢٨ مايو ٢٠١٤ أطلقت كاسبر سكاي خدمة تفاعلية جديدة Cyber Threat Map تظهر الحوادث الإلكترونية التي تحدث في العالم في ذات لحظة وقوع الحادثة[٨٠]، ويهتم موقعKasper Sky. Cyber stat. com اهتماماً خاصاً بالتهديدات الإلكترونية ومسبباتها وتحديد البرمجيات الخبيثة الأنشط من غيرها، كما يقدم الموقع تصنيفاً للتهديدات الأكثر انتشاراً وقوائم الدول الأكثر تهديداً.

قامت دولة الإمارات العربية المتحدة بتقوية أمنها الإلكتروني، وترتب على ذلك أن أحتلت المرتبة الأولى في دول مجلس التعاون الخليجي ، والمرتبة الرابعة على مستوى العالم في العام ٢٠١٢ في مجال الأمن الإلكتروني وفقاً لتقرير صادر عن المعهد الدولي للتنمية الإدارية[٨١]، بينما كان ترتيب دولة الإمارات في العام ٢٠١١ في المرتبة الخامسة والثلاثين، ووفقاً لتقرير مؤشر الأمن الإلكتروني العام الصادر عام ٢٠١٣ فقد احتلت سلطنة عمان المركز الأول.

نخلص الى نتيجة مفادها ارتفاع معدلات الجرائم الإلكترونية في دول مجلس التعاون الخليجي حيث ذكر نائب القائد العام لشرطة دبي بأن الجرائم الالكترونية والاقتصادية تعتبر ابرز الظواهر الإجرامية الحديثة على المجتمعات الخليجية، وتحديداً المجتمع الإماراتي، حيث لم يكن هذا النوع من الجرائم معروفاً أو موجوداً قبل ٤٠ عاماً، لاسيما وقد أشار نائب القائد لشرطة دبي خلو مضابط الشرطة من هذا التصنيف الجرمي، كما أشار إلي مضاعفة أعداد هذه الجرائم خلال السنوات الماضية، حيث كانت ٢٧٨ بلاغاً في العام ٢٠٠٨ وبلغ الإحصاء ٤٣٦ في العام ٢٠٠٩، وتصاعدت الى ٤٤٥في العام ٢٠١٠ وتصاعد العدد في العام ٢٠١١ الى ٥٨٨ بلاغاً ، وزادت نسبة الجريمة كذلك في الأعوام ٢٠١٢ وبلغ عدد الجرائم ٧٧٢ ، وفي العام ٢٠١٣ تجاوز العدد ١٠٠٠ بلاغ.[٨٢]

وكذلك الحال في بقية دول الخليج العربي حيث تزداد نسبة الجريمة بصورة متسارعة وكذلك يلاحظ أن أنماط الجريمة الإلكترونية في دول مجلس التعاون الخليجي تنصب غالباً في الجرائم المالية حيث تستهدف الشركات والمؤسسات الاقتصادية والمالية، و يستهدف القراصنة بعض المواقع الرسمية والحكومية للدول، وهناك أيضاً الرسائل غير المرغوبة التي تتم عبر وسائل التواصل الاجتماعي حيث بلغت ٧٩٪ في المملكة العربية السعودية.[٨٣]

٨٠ Kasper Sky.com/news=9074/24 sepal- 2014

٨١ _www.nxme.net /information

٨٢ جريدة الاتحاد الإماراتية، بتاريخ ٢٣ فبراير ٢٠١٣.

٨٣ Symantec- Internet Security Threats.

المطلب الثاني
وسائل مكافحة الجريمة الإلكترونية

لتحديد تحديات الجريمة الإلكترونية، ينبغي أولاً أن نحدد الفرق بين الجرائم التي ترتكب بواسطة شبكة المعلومات العالمية، بالمعنى الفني الدقيق، وبقية الجرائم التي تستخدم فيها الشبكة العالمية للمعلومات، أو أي أجهزة من أجهزة تقانة المعلومات كأداة لارتكابها. ويتبين من الطبيعة الخاصة بالجريمة أنها تتميز وتتسم بمجموعة من الخصائص التي تتولد عنها تحديات عديدة يترتب عليها صعوبة التعامل مع هذه الجرائم وضبطها.

وسائل مكافحة الجريمة الإلكترونية:

١- إصدار التشريعات المواكبة لتطورات الجريمة الإلكترونية وانسجام التشريعات الوطنية مع الاتفاقيات والقواعد الدولية والقوانين المقارنة ذات الصلة لتمكين أجهزة العدالة الجنائية من أداء دورها على النطاق الوطني والإقليمي والدولي بالصورة التي تسهم بالمكافحة الفعالة للجريمة الإلكترونية.

٢- رفع كفاءة الأجهزة التقنية المختصة برصد التهديدات والمخاطر والتبليغ بالإنذار المبكر وتزويدها بأحدث المعدات.

٣- تدريب وتأهيل الفنيين والمهندسين العاملين في مجال الأدلة الرقمية وترشيد وتطوير أدائهم.

٤- تدريب وتأهيل المختصين بأجهزة العدالة الجنائية على كيفية التعامل مع الأدلة الرقمية.

٥- إتباع كافة وسائل التوعية الأمنية للحد من مخاطر الجريمة الإلكترونية.

ويقصد بالدور الفني إتباع اساليب المكافحة الإلكترونية للجرائم من خلال الاستخدام الأمثل للوسائل التكنولوجية والإلكترونية المتمثلة في نظم الحاسبات الآلية والاتصالات متلازمتين.

صعوبة مكافحة الجرائم الإلكترونية:

من أهم صعوبات مكافحة الجرائم الإلكترونية:

أ- عدم كفاية القوانين ومواكبتها للتطورات التقنية في كثير من الدول.

ب- احجام الكثير من الجهات التبليغ عن تلك الجرائم.

ج- سهولة إخفاء معالم الجريمة.

د- عدم وجود دليل مادي واضح.

هـ- صعوبة الوصول إلى الدليل في بعض الأحيان.

و- وجود كم هائل من المعلومات بتعيين فحصها.

أولاً: الصعوبات على المستوى الوطني:

تتعدد الصعوبات التي تواجه الدور الذي تقوم به الأجهزة الأمنية في مكافحة الجرائم الإلكترونية على المستوى الوطني، وأهم هذه الصعوبات تتمثل في:

أ- عدم كفاية القوانين الحالية: هذا التطور المتلاحق في مجال تقنية المعلومات والاتصالات يقابله استغلال الجناة لهذه التقنية المتطورة بابتكار أساليب جديدة لارتكاب الجرائم الإلكترونية، ولذلك يتطلب الأمر مواكبة القوانين لهذه التطورات واستيعابها.

ب- أحجام الكثير من الجهات عن التبليغ عن تلك الجرائم: يهدف هذا الأحجام من قبل هذه الجهات إلى عدم الإساءة لطبيعة عمل المنشأة، وعدم بيان عجزها عن تحقيق الأمان الكافي للمعلومات، وبالتالي لأصول الأموال التي تتعامل معها، وقد يكون لذلك مردود سيء لدى العملاء الذين ربما يلجأ كثير منهم لسحب أموالهم ووقف تعاملاتهم مع المنشأة.

ج- سهولة إخفاء معالم الجريمة: ويتمثل ذلك في عدم معرفة مصدر مرتكب الفعل، بحيث إذا تم ارتكاب الفعل وظهرت نتيجته بعد فترة زمنية، مثل قيام شخص ما بزرع برنامج فيروسي يكتشف بعد تحقق آثاره التدميرية والسالبة.

د- عدم وجود دليل مادي واضح: الدليل المادي الذي يتوافر قد يكون في الغالب أوراق متحصلة من الطابعة من خلال الجهاز والدليل هنا يكون الأوراق المتحصلة وليس ما يحويه الجهاز في حد ذاته.

هـ- صعوبة الوصول إلى الدليل في بعض الأحيان: الدليل في الجريمة الإلكترونية عبارة عن معلومات قد تحاط بوسائل فنية لحمايتها، وتلك الوسائل قد تكون عائقاً أمام عملية البحث والتحري والاطلاع.

و- وجود كم كبير من المعلومات يتعين فحصها: يتطلب البحث عن معلومات تفيد في كشف أدلة جريمة معينة البحث في كم كبير من الملفات والبرامج المخزنة والتي قد يكون لها ارتباط بمعلومات خاصة بارتكاب الجريمة.

ثانياً: الصعوبات على المستوى الدولي:

يمكن تفصيل الصعوبات على المستوى الدولي كالتالي:

أ- اختلاف مفاهيم الجريمة لاختلاف التقاليد القانونية وفلسفة النظم القانونية.

ب- عدم التناسق في القوانين الإجرائية فيما يتعلق بالتحري والتحقيق في الجرائم الإلكترونية.

ج -عدم وجود الخبرة الكافية لدى الأجهزة الأمنية والعدلية لتمحيص عناصر الجريمة.

د- عدم كفاية الاتفاقيات الدولية والثنائية في مجال تسليم المجرمين.

التدابير الأمنية في التعامل مع الجريمة الإلكترونية:

تشتمل الإجراءات الأمنية على مجموعة من التدابير، وبالضرورة يجب التمييز بين مرحلة ما قبل وقوع الجريمة ومرحلة ما بعد وقوعها.

أولاً: تدابير مرحلة ما قبل وقوع الجريمة الإلكترونية (أمن المعلومات):

تشمل كافة الإجراءات التي تتخذ وبمشاركة كافة القطاعات وهو ما يطلق عليه أمن المعلومات، والقواعد التي تحكم أمن المعلومات تشمل:

أ- تحديد المعلومات الهامة.

ب- تحليل المخاطر والتهديدات.

ج- تحليل القابلية للعدوان.

د- تطبيق الإجراءات المضادة.

هـ- التقييم ودراسة الأساليب والإجراءات المضادة.

ثانياً: تدابير مرحلة ما بعد وقوع الجريمة الإلكترونية:

تعتبر المواجهة السريعة للجريمة الإلكترونية ضرورة هامة، حيث أنه كلما استغرقت المواجهة وقتاً طويلاً، ترتب على ذلك مشكلات قد تعوق الكشف عن الجريمة، يتم استعراض كيفية مواجهة تلك الجرائم الإلكترونية من خلال:

أ- تحديد فريق التصدي لمكافحة الجريمة.

ب- تحديد أسلوب عمل فريق التصدي لمكافحة الجريمة.

ثالثاً: الحماية والتأمين بالوسائل التقنية:[٨٤]

ويتم ذلك على أربعة مستويات هي:

أ- تأمين وحماية الحاسبات الشخصية والحاسبات الخادمة.

ب- تأمين وحماية شبكة الربط بالإنترنت.

ج- تأمين المعلومات المتداولة.

د- الحماية من التهديدات والاختراقات.

رابعاً: التأمين بوضع السياسة الأمنية:[٨٥]

ويتم ذلك عبر المحاور التالية:

أ- أمن الأفراد.

ب- التأمين الطبيعي.

ج- تحديد الهياكل التنظيمية المساندة (كيان الأمن).

د- تصنيف المصادر العملياتية والبيانات والمعلومات.

هـ- تحديد مستويات الدخول وأحقيات التعامل.

و- تأمين عمليات التشغيل.

ز- تأمين التطبيقات والشبكات والخدمات (كالبريد الإلكتروني ونقل الملفات والتجارة الإلكترونية ... وغيرها).

ح- تأمين مراحل تطوير النظم وتشتمل (تجميع البيانات والتحليل والتصميم والبرمجة والتشغيل والصيانة والدعم الفني).

ط- إدارة وتحليل المخاطر وتحديد خطط استمرارية العمل.

ى- الالتزام بتشريع تأمين الحماية للبيانات على المستوى القومي.

المستوى الأول للحماية والتأمين بالوسائل التقنية ينصب على تأمين وحماية الحاسبات الشخصية والحاسبات الخادمة وهي تمثل من وجهة نظر الباحث أهم المستويات للتأمين والحماية، حيث يمكن حماية هذه الحاسبات الشخصية والخادمة بالأساليب التالية:

---

٨٤ د. أحمد الشربجي، د. وقائي بغدادي: حماية وتأمين الإنترنت التحدي القادم وأساليب المواجهة، سلسل العلوم والتكنولوجيا، الهيئة المصرية العامة للكتاب، القاهرة، ٢٠١٠، ص١٥٦.

٨٥ المرجع السابق، ص١٥٨.

أ- الحماية المادية: وهي ما يعرف بالحماية الطبيعية، كأن يتم وضع الأجهزة في غرف مؤمنة بعيداً عن مخاطر العابثين والمتصنتين وغيرهم، وذلك إما بحراسة فعلية أو بأقفال إلكترونية أو بغيرها.

ب- الحماية بتعريف هوية المستخدم: وتشمل استخدام البصمة للمستخدم، أو البطاقة الذكية للدخول وغيرها من أدوات تعريف هوية المستخدم كاستخدام كلمة المرور.

ج- الحماية بالتحصين وتعديل البرامج التشغيلية بهدف سد الثغرات الأمنية التي يتم اكتشافها في برامج التشغيل.

د- الحماية بأغلاق الأجهزة والشاشات غير المستخدمة: من أهم واجبات إجراءات السياسة الأمنية ضرورة التنبيه على المستخدمين بأغلاق أجهزتهم عند خروجهم من المكاتب.

ينبغي مراعاة الآتي عند وضع السياسة الأمنية لشبكات المعلومات:

أ- الهدف الأساسي هو تقديم سياسة متكاملة للتأمين والحماية.

ب- التأمين والحماية من أهم الخدمات التي يوفرها النظام.

ج- سياسة التأمين والحماية يجب أن تكون ديناميكية متغيرة مع كل استحداث لأساليب الاختراق.

نخلص إلى أن الوقاية من الجريمة الإلكترونية تتطلب الآتي:[٨٦]

أ- استخدام كلمات مرور لا يمكن الوصول إليها. Strong Passwords

ب- تأمين جهاز الحاسوب الخاص من خلال:

١- تفعيل برامج الحماية مثل : (الجدران النارية).Fire wall

٢- استخدام مضادات الفيروسات. anti virus

٣- التحديث المستمر لبرامج مكافحة التجسس. Anti Spyware

ج- ضبط التعامل مع وسائل التواصل الاجتماعي.

د- تحديث منظم التشغيل للحاسوب الخاص بصورة دائمة منعاً للاختراق والتجسس.

هـ- إيجاد أقصى درجات الحماية للبيانات.

---

٨٦ Royal Canadian Touted Police- www.ramp-grc/Cyber-tips conceals- Eng. Hem

لمزيد من المعلومات يراجع: Get Cyber Saps

و- تأمين الشبكة اللاسلكية الخاصة (Wi-Fi) وتحديث الاعدادات الخاصة بها، مع تجنب إجراء المعاملات المالية عليها.

ز- حماية البيانات المتعلقة بالبريد الإلكتروني في مجالات استخدام المعاملات المالية وغيرها.

ح- تجنب الأخطاء الناتجة عن عدم معرفة التعامل مع الحاسوب.

ط- الاتصال بالجهات الرسمية عند وقوع المستخدم ضحية لتجسس أو اختراق.

التعاون الدولي في مواجهة الجريمة الإلكترونية:

تسهم الجهود الدولية والإقليمية في مكافحة الجريمة الإلكترونية بالوسائل المختلفة، ويتم تناول هذا الجانب بالتفصيل المناسب في المبحث الرابع.

المبحث الثالث
مدى تأثير شبكات التواصل الاجتماعي على مجتمع دول مجلس التعاون لدول الخليج العربية

نتناول موضوعات هذا المبحث في مطلبين كما يلي:

المطلب الأول: ماهية شبكات التواصل الاجتماعي وأنواعها ومميزاتها ونماذجها.

المطلب الثاني: استخدامات شبكات التواصل الاجتماعي وآثارها.

المطلب الأول
ماهية شبكات التواصل الاجتماعي وأنواعها ومميزاتها ونماذجها

تعريف شبكات التواصل الاجتماعي:

تناول كثير من فقهاء تقنية المعلومات مفهوم الشبكات الاجتماعية المرتبطة بالمعلوماتية، كما تناولها فقهاء الفكر القانوني والاجتماعي والإداري والاستراتيجي والاقتصادي وغيرهم بالتعريف كل من خلال نظرتهم وتخصصهم.

فقد تناولها فايز الشمري بالتعريف بأنها نظام المعلومات العالمي الذي يتصل ببعضه بواسطة عناوين متفردة معتمدة على بروتوكول الانترنت أو لواحقه وتوابعه الفرعية [٨٧].

كما عرفها علي عسيري بأنها وسيط ناقل للمعلومات بين أجهزة الكمبيوتر المتصلة به بواسطة أنظمة تحكم في البيانات وبروتوكولات وعناوين خاصة [٨٨].

وعرفها عبد الله الغامدي بأنها مجموعة من الحواسيب مرتبطة ببعضها لتكون شبكة عالمية وشبكات اتصال[٨٩].

وهناك تعريف مشعل القدهي على أنها عبارة عن مئات الملايين من الحاسبات الآلية حول

---

٨٧ فايز الشمري: استخدامات شبكة الإنترنت في الإعلام العربي ، مجلة البحوث الأمنية كلية الملك فهد العدد التاسع عشر شعبان ١٤٢٢هـ .

٨٨ علي بن عبدالله عسيري: الآثار الأمنية لاستخدام الشباب للإنترنت ، مركز الدراسات والبحوث – جامعة نايف العربية للعلوم الأمنية، الطبعة الأولى ١٤٢٥ هـ

٨٩ عبدالله بن أحمد الغامدي: تردد المراهقين على مقاهي الانترنت وعلاقته ببعض المشكلات لدى عينة من طلاب المرحلة الثانوية بمكة المكرمة ، رسالة الماجستير – جامعة أم القرى، ١٤٢٩هـ .

العالم مرتبطة ببعضها يمكن إرسال الرسائل الالكترونية بينها في لمح البصر بالإضافة إلى تبادل الملفات والصور والأحداث[٩٠].

من التعاريف السابقة يمكن استنباط مميزات شبكات التواصل الاجتماعي التي تشمل وتتضمن :

١- أنه نظام عالمي خارج حدود المنطقة والدولة .

٢- إنه عالم افتراضي تقني .

٣- أنه يعتمد على بروتوكولات لنقل المعلومات .

٤- الاتصال يتم من خلال عناوين خاصة وأجهزة إلكترونية .

من خلال ما ذكر أعلاه يمكننا أن نستنبط تعريفاً لشبكات التواصل الاجتماعية بأنها مجموعة المواقع على شبكة المعلومات الدولية (الإنترنت) تتيح التواصل بين الأفراد في بيئة مجتمع افتراضي يجمعهم الاهتمام أو الانتماء لبلد أو مدرسة أو فئة معينة في نظام عالمي لنقل المعلومات.

يتبين من خلال التعريف أعلاه أن شبكات التواصل الاجتماعي تتميز عن غيرها من المواقع في الشبكة الإلكترونية بعدة ميزات أبرزها:

١- أن هدف المواقع الاجتماعية خلق جو من التواصل في مجتمع افتراضي تقني يجمع مجموعة من الأشخاص من مناطق ودول مختلفة على موقع واحد تختلف وجهاتهم ومستوياتهم وتتفق لغتهم التقنية.

٢- أن الاجتماع يكون على وحدة الهدف سواء التعارف أو التعاون أو التشاور أو لمجرد الترفيه فقط وتكوين علاقات جديدة أو استطلاع واكتشاف.

٣- إن الشخص في هذا المجتمع عضو فاعل بمعنى أنه يرسل ويستقبل كتابة وحديثاً حيث يتجاوز دور الاستماع والاطلاع فقط، أما دور صاحب الموقع (Administration) هو الرقيب والموجه للتواصل الإيجابي.

---

٩٠ مشعل عبدالله القدهي: المواقع الاباحية على شبكة الانترنت وأثرها على الفرد والمجتمع، مدينة الملك عبد العزيز للعلوم والتقنية .

أنواع الشبكات الاجتماعية[٩١]:

يمكن تقسيم الشبكات الاجتماعية وفقاً للهدف من إنشائها أو تبعاً للخدمة المقدمة، حيث يمكن تقسيمها إلى الأنواع التالية:

أ- شبكات شخصية: وهي شبكات لشخصيات محددة أو أفراد أو مجموعة أشخاص أصدقاء تمكنهم من التعارف وإنشاء صداقات بينهم، مثل (Facebook).

ب- شبكات ثقافية: تختص بفن معين وتجمع المهتمين بموضوع أو علم معين .

ج- شبكات مهنية: تهتم وتجمع أصحاب المهنة المتشابهة لخلق بيئة تعليمية أو تدريبية فاعلة، مثل (LinkedIn).

كما يمكن تقسيم الشبكات الاجتماعية أيضاً وفقاً للخدمات وطريقة التواصل إلى الأنواع التالية:

أ- شبكات تتيح التواصل الكتابي.

ب- شبكات تتيح التواصل الصوتي.

ج- شبكات تتيح التواصل المرئي.

هناك أيضاً تقسيم ثالث يقسم الشبكات الاجتماعية إلى:

أ- شبكات داخلية خاصة: (Internal Social Networking). وتتكون من مجموعة من الناس تمثل مجتمع مغلق أو خاص يمثل الأفراد داخل شركة أو مؤسسة تعليمية أو منظمة أو أي تجمع ويتم التحكم في دعوة هؤلاء الأشخاص دون غيرهم للدخول للموقع والمشاركة فيه من تدوين وتبادل الآراء وملفات ومناقشات مباشرة وغيرها مثل شبكة (LinkedIn).

ب- شبكات خارجية عامة: (Extern at Social Networking). وهي شبكات متاحة لجميع مستخدمي الانترنت بل صممت لجذب المشتركين المستخدمين للشبكة بالمشاركة في الأنشطة بمجرد التسجيل في الموقع وتقديم أنفسهم مثل شبكة (face book) و (Twitter) وغيرها.

---

٩١ http://www.alukah.net/culture/0/59302

مميزات شبكات التواصل الاجتماعي:

تتميز شبكات التواصل الاجتماعي بعدة مميزات منها[٩٢]:

١- العالمية: حيث تلغي الحواجز الجغرافية والمكانية وتعبر الحدود الدولية بلا استئذان حيث يستطيع الفرد التواصل أينما كان موقعه بكل سهولة مع الآخرين.

٢- التفاعلية: فالفرد في شبكة التواصل الاجتماعي مستقبل وقارئ ومشارك في آن واحد، هذه الميزة تلغي الجانب السلبي في وسائل الأعلام التقليدية التي لا تتيح المشاركة المباشرة.

٣- تعدد الاستعمالات: حيث يمكن أن يستخدمها المستقبل لتلقي الخدمة أو المرسل للتواصل مع الآخرين.

٤- سهولة الاستخدام: شبكات التواصل الاجتماعي تستخدم بالإضافة للحروف وبساطة اللغة فإنها تستخدم الرموز والصور وغيرها التي تسهل عملية التفاعل بين المستخدمين.

٥- التكلفة الاقتصادية: شبكات التواصل الاجتماعي اقتصادية في الجهد والوقت والمال فهي في معظم برامجها مجانية الاشتراك والتسجيل حيث يستطيع الجميع امتلاك جزء من شبكة التواصل الاجتماعي وليست حكراً على أصحاب الأموال أو حكراً بجماعة دون غيرها.

نماذج وصور شبكات التواصل الاجتماعي:

يمكن أن نشير إلى بعض نماذج وصور لشبكات التواصل الاجتماعي الموجودة على الإنترنت والتي تتميز بسعة الانتشار وخاصة على مستوى دول منطقة الخليج العربي محل البحث، فهي تشمل[٩٣]:

أولاً: الفيس بوك Face book

يعد موقع الفيس بوك أحد أشهر المواقع على شبكة الإنترنت ورائد التواصل الاجتماعي حيث يعتبر منبر للتعبير ويتعامل به كل قطاعات المجتمع شيباً وشباباً وبمختلف الأعمار، وهو موقع يساعد على تكوين علاقات بين المستخدمين يمكنهم من تبادل المعلومات والملفات والصور الشخصية ومقاطع الفيديو والتعليقات وكل هذا يتم في عالم افتراضي يقطع حاجز الزمان والمكان.

---

٩٢ http://www.alukah.net/publications-competitions/0/404

٩٣ http://lljk599.blogspot.com/2014/04/blog-post-6251.html

ثانياً: تويتر twitter

موقع تواصل اجتماعي يقدم خدمة تسمح لمستخدميه بإرسال تحديثات Tweets عن حالتهم من خلال رسائل أو رسائل قصيرة S.M.S أو برامج المحادثة الفورية وغيرها، حيث تظهر تلك التحديثات في صفحة المستخدم ويمكن للأصدقاء الآخرين قراءتها مباشرة من صفحتهم الرئيسية أو من ملف المستخدم وكذلك يمكن استقبال الردود والتحديثات.

ثالثاً: المدونات Web blogs

هي مواقع شخصية على الإنترنت تساعد الأفراد على التفاعل من خلال المشاركة والتعلم عبر تبادل الأفكار والمعلومات، من مميزاتها:

أ- سهولة الإنشاء حيث هناك الكثير من البرامج الجاهزة التي تساعد في التصميم.

ب- سهولة التدوين والنشر.

ج- كسر حواجز الزمان والمكان حيث يمكن التدوين في أي وقت.

د- إمكانية حفظ الحقوق للأفكار والتحديثات.

هـ- إمكانية التفاعل مع الآخرين Feed back من خلال الردود المباشرة.

و- التوفير في الوقت والجهد في التدوين والتوزيع مع المحافظة على البيئة.

ز- إمكانية التدوين بطريقة منظمة تمكن من الحصول على المعلومات بكل سهولة.

ح- إمكانية استخدام الصوتيات والمرئيات.

ط- مساحة حرة للاستخدام.

رابعاً: واتسب WhatsApp

موقع للتواصل الاجتماعي، عبارة عن شبكة إلكترونية تسمح للمستخدم إنشاء موقع خاص به مع إمكانية ربطه بالمواقع الأخرى التابعة للأصدقاء وهو برنامج يعمل على الهواتف الذكية، وما يميزه أنه يتيح إمكانية التعديل على المواد التي يتم تداولها ويسمح للمستخدمين بالمشاركة المباشرة.

المطلب الثاني
استخدامات شبكات التواصل الاجتماعي

هناك استخدامات عديدة لشبكات التواصل الاجتماعي منها الاستخدامات الايجابية ذات الأثر الايجابي ومنها أيضاً الاستخدامات السالبة أو ذات الأثر السلبي.(٩٤)

أولاً: الاستخدامات الايجابية لشبكات التواصل الاجتماعي:

يمكن الاستفادة من شبكات التواصل الاجتماعي في الجوانب الايجابية التالية:

١– استخدامات الاتصالات الشخصية:

وهو الاستخدام الأكثر شيوعاً حيث يمكن من خلالها تبادل المعلومات والملفات الخاصة والصور ومقاطع الفيديو، كما أنها مجال رحب للتعارف والصداقة، وخلق مجتمع يتميز بوحدة الأفكار والرغبات وإن اختلفت أعمارهم وأماكنهم ومستوياتهم العلمية.

٢– الاستخدامات التعليمية:

هناك دور هام تلعبه شبكات التواصل الاجتماعي في مجال تطوير التعليم الإلكتروني وتعمل على إضافة الجانب الاجتماعي له بمشاركة كل الأطراف في منظومة التعليم كالمدرسة أو الجامعة والمنزل.

٣– الاستخدامات الحكومية:

اتجهت كثير من الدوائر والوحدات الحكومية للتواصل مع الجمهور متلقي الخدمة الحكومية من خلال موقع التواصل الاجتماعي بهدف قياس وتطوير الخدمات حيث تتميز هذه الخدمة بقلة تكلفتها والوصول المباشر للمستفيد مع إمكانية التعامل والتفاعل Feed back بين الأطراف.

٤– الاستخدامات الإخبارية:

حيث أصبحت شبكات التواصل الاجتماعي مصدر أصيل من مصادر الأخبار لكثير من روادها.

٥– الاستخدامات الدعوية:

فتحت شبكات التواصل الاجتماعي الباب للتواصل والدعوة مع الآخرين بمختلف معتقداتهم ولغاتهم وأصبح للكثير من الدعاة مواقعهم الالكترونية وهو ما يمثل انتقال ايجابي

٩٤ http://www.almaaref.org/books/contentsimages/books/zad-almobalegh /zad-alrahma-fe-shahr-alla h/page/lesson14. htm

للتواصل العالمي بعيداً عن الوسائل التقليدية حيث تتميز الدعوى عن طريق شبكات التواصل الاجتماعي بالعالمية والفورية مع التوفير في الجهد والوقت والتكاليف.

ثانياً: الاستخدامات السلبية لشبكات التواصل الاجتماعي.

كما لشبكات التواصل الاجتماعية جوانب ايجابية عديدة قابلة للتطوير والتوظيف الفعال هناك أيضاً الجوانب المظلمة والسالبة في هذه الشبكات الاجتماعية.

هناك بعض صور الاستخدامات السالبة تشمل على سبيل المثال:

١- بث الأفكار الهدامة والدعوات المنحرفة والتجمعات المخالفة للقيم والقانون.

٢- عرض المواد الإباحية والفاضحة الخادشة للحياء العام.

٣- التشهير والمضايقة وبث الإشاعات.

٤- التحايل والابتزاز والتزوير.

٥- انتهاك الحقوق الخاصة والعامة.

٦- الاستغلال الجنسي للأطفال.

تجارب ناجحة للاستخدامات الايجابية للشبكات الاجتماعية.

هناك تجارب ناجحة للاستخدامات الايجابية للشبكات الاجتماعية منها:

١- التجارب الاجتماعية: كتلك التي يتم فيها التواصل بين الأفراد في الدولة أو على مستوى الأسرة والقبيلة في تواصل يعزز قوة المجتمع. ويلاحظ أن الاتجاه العام لاستخدام الشبكة الاجتماعية دون عصبية أو ازدراء للآخرين.

٢- التجارب العلمية: تؤكد التحديات المعاصرة على أهمية توظف أجهزة الرقابة في أنشطة التعليم والتعلم والواقع يؤكد تدفق المعلومات عبر الشبكة مكوناً مجتمع المعلومات (Information community).

٣- التجارب الدعوية: هناك الكثير من الدعاة أتجه للتواصل مع الآخرين من خلال الشبكات الاجتماعية وإمكانياتها وتوظيفها، وهذه التجارب تحسب إيجاباً لصالح الشبكات الاجتماعية والتي يمكن ملاحظة نموها السريع المضطرد.

من خلال الطرح السابق نخلص إلى أن الشبكات الاجتماعية شبكات عالمية للتواصل بين أجهزة متعددة في نظام عالمي لنقل المعلومات، وتتميز أيضاً الشبكات الاقتصادية أنها عالمية

خارج حدود الزمان والمكان ويمكن الاستفادة منها في خدمات التواصل الشخصي أو التعليمي أو الدعوي أو الإخباري أو الحكومي أو الرسمي.

مستخدمو مواقع التواصل الاجتماعي الإلكترونية في دول مجلس الخليج العربي:

وفقاً لموقع مركز الرياض للمعلومات والدراسات الاستشارية فقد صدر تقرير المركز المالي الكويتي[٩٥] حول مواقع التواصل الاجتماعي الالكترونية في دول مجلس التعاون الخليجي، تناول الاتجاهات العامة لاستخدام مواقع التواصل الاجتماعي، كما أبرز التقرير محفزات النمو والفرص والتحديات الرئيسية لهذا القطاع. وفقاً للتقرير فقد تصدرت المملكة العربية السعودية والأمارات قائمة مجموعة دول مجلس التعاون الخليجي الأكثر استخداماً لمواقع التواصل الاجتماعي، وقد بلغ مجموع مستخدمي موقع Facebook وحده أكثر من (١٦) ستة عشر مليون مستخدم في دول الخليج العربي وأصبحت الشركات في الخليج العربي أكثر إدراكاً للتسوق عبر وسائل التواصل الاجتماعي وكذلك في مجال الترفيه الإلكتروني.

كما أشار التقرير إلى أن نسبة السكان الشباب دون سن ٣٥سنة تبلغ ٦٧٪من مجموع عدد سكان دول مجلس التعاون وهي نسبة تزيد عن المتوسط العالمي، مما يترتب على ذلك إسهام هذه الشريحة السكانية الشبابية في تسريع وانتشار الاستخدام لوسائل التواصل الاجتماعي مع وضع في الاعتبار انتشار الهواتف النقالة الذكية وانتشار الإنترنت بسرعة متزايدة وبمعدل نمو سنوي مركب يبلغ ١٥٪، لاسيما وأن التقرير يشير إلى توقع زيادة الإنفاق الحكومي على قطاع تقنية المعلومات.

وعلى الرغم من أن استخدام الشباب لمواقع التواصل الاجتماعي كان في البداية لأغراض الدردشة وإقامة العلاقات والصداقات وتفريغ الشحنات العاطفية، إلاّ أنه وبمرور الوقت تطورت العلاقات بين الشباب ومواقع التواصل الاجتماعي وصار الاستخدام في مجالات تبادل وجهات النظر وتحسين الأوضاع الاجتماعية والاقتصادية والسياسية كما يتم النقل فيها للإحداث لحظة بلحظة مما يمكن أن نؤكد بأن مواقع التواصل الاجتماعي كانت سبباً في:

١- إتاحة الفرصة للشباب للتواصل بشكل أكبر.

٢- ساهمت في إضافة النضج إلى تعاملات وتصرفات الشباب.

٣- ساهمت في إعطاء الشباب الفرصة للتعبير عن آرائهم.

٩٥ وأنظر الملحق رقم (٦) ص ب، والموقع الإلكتروني التالي:http://www.alriyadh.com/980890

وقد نشرت صحيفة الأنباء الكويتية (٢٥ نوفمبر ٢٠١٣م) أن الكويت أصبحت من أكثر الدول الخليجية استخداماً لوسائل التواصل الاجتماعي حيث تحولت مواقع التواصل الاجتماعي إلى مشروعات تجارية واستثمارية مما جعل البعض يفكر في فرض ضرائب على تلك المشروعات وخاصة المشروعات التي تستخدم برنامج للتواصل.[٩٦]

الآثار السلبية لاستخدام مواقع التواصل الاجتماعي وتفشي الفساد الأسري:

تعددت وتنوعت الدراسات التي تهتم بتحليل ظاهرة وأسباب الفساد الأسري، وقد أشارت تلك الدراسات إلى كثير من التسهيلات التي قدمتها تقنيات التواصل الاجتماعي، وساهمت بها في نشر الفساد من خلال:

١- الاستلاب الثقافي واختلاط القيم الأخلاقية.

٢- تفشي تقنيات العولمة ذات التأثير على الأخلاقيات.

٣- عدم السيطرة على استخدامات أجهزة تقنية المعلومات.

ولا شك أن النقاط أعلاه ذات تداخل كثيف فيما بينها وذات صلة وثيقة بموضوع تفشي الفساد الأسري من خلال مواقع التواصل الاجتماعي الالكترونية، حيث تتداخل التقنية المعلوماتية مع أدق الخصوصيات بل وصارت الصور الجنسية هي المحور في مواقع التواصل الاجتماعي وهو ما يندرج تحت ما يعرف بالاستغلال والتحرش الجنسي.

وعلى الرغم من الإيجابيات الهائلة لشبكة الانترنت بصورة عامة والايجابيات العديدة لمواقع التواصل الاجتماعي، إلا أن المخاطر الناجمة عن هذه الشبكات بالغة الحدة والعمق خاصة بالنسبة لصغار السن أو ما يعرف بفئة الأحداث محدودي المعرفة قليلي الخبرة لاسيما وأن الأحداث وصغار السن يتميزون بالميل للمخاطرة والرغبة في التقليد والانجذاب للجنس الآخر والسعي نحو المغامرة واثبات الذات، و الشبكة العالمية للمعلومات ومواقع التواصل الاجتماعي الالكترونية تتضمن العديد من المخاطر التي يكون لها أعمق الأثر على فئة صغار السن، ومن أبرز تلك المخاطر:

١- دخول المواقع الإباحية.

٢- المعاكسة من خلال البريد الإلكتروني.

٩٦ http://www.kolalwatn.net/news136120

٣- الاطلاع غير المصرح على أسرار الغير.

٤- اللهو غير البريء.

٥- الاطلاع على المطبوعات الممنوعة.

٦- التأثر بالأفكار المتطرفة والهدامة.

٧- اكتساب الخبرات السالبة.

٨- الميل نحو الانعزال.

٩- الإجرام الإلكتروني.

وبحلول منتصف العام ٢٠١٤م كان هناك ما يزيد عن ٧١ مليون مستخدم نشط لوسائل التواصل الاجتماعي من بين ١٣٥مليون مستخدم للإنترنت في العالم العربي متضمناً مجتمعات دول مجلس التعاون الخليجي . وقد باتت هذه المواقع الاجتماعية وسائل أساسية للخدمات التي تقدم سواء عبر القطاع الخاص أو القطاع الحكومي.[٩٧]

ووفقا لنتائج تقرير الإعلام الاجتماعي العربي السادس الصادر عن برنامج الحوكمة والابتكار في كلية محمد بن راشد للإدارة الحكومية[٩٨] والذي جاء تحت عنوان ''إشراك المواطنين والخدمات العامة في العالم العربي: إمكانيات الإعلام الاجتماعي''، فإن استخدام وسائل التواصل الاجتماعي تزايد بشكل مضطرد في العالم العربي، إذ ارتفعت أعداد مستخدميها منذ مايو ٢٠١٤ بنسبة ٤٩٪ لموقع فيسبوك و٥٤٪ لموقع تويتر و٧٩٪ لموقع لنكد إن. وكشف التقرير أن دولة الإمارات تمتلك أعلى نسبة انتشار لمستخدمي لنكد إن بالنسبة لعدد السكان والتي وصلت إلى ٢٢,٤٪ بينما تتصدر قطر ترتيب نسبة انتشار فيسبوك مع ٦١٪ من سكانها ينشطون على الموقع وتليها الإمارات بفارق بسيط بنسبة ٥٨٪، أما على موقع تويتر فتمتلك السعودية أكبر عدد من المستخدمين يمثلون ٤٠٪ من إجمالي مستخدمي الموقع النشطين في العالم العربي ولكن الكويت تحتل المرتبة الأولى في نسبة الانتشار مع ١١,٤٪ من سكانها يمتلكون حسابات نشطة على تويتر.

نستنتج من ذلك التنامي المستمر لوسائل الاتصال الاجتماعي في المنطقة العربية، وبصفة

---

٩٧ http://www.mbrsg.ae/getattachment/9cea0fcc-9e43-4fba-9f47-ea6d9d16ca8c/Arab-Social-Media-Outlook 2014.aspx

٩٨ http://arabic.arabianbusiness.com/politicseconomics/society/2014/jun/25/364833/#.VK5jWujTHAw

خاصة في المنطقة الخليجية والتأثيرات التي يمكن أن تحدثها في مختلف أوجه حياة المواطن في دول مجلس التعاون الخليجي وبصفة خاصة فئة الشباب، الأمر الذي يتطلب تكاتف جميع مؤسسات التنشئة الاجتماعية ومؤسسات المجتمع المدني ووسائل الإعلام للتصدي لهذا الجانب.

المبحث الرابع
التعاون الدولي والاقليمي لمواجهة الجريمة الإلكترونية

مقدمة:

أدت التطورات المتلاحقة في علوم الحاسب الآلي وتقنية المعلومات وشبكة الانترنت إلى نقلة علمية وتطبيقية حضارية إيجابية هائلة في كافة مجالات الحياة ، ومع الاستخدام المكثف لشبكة الإنترنت ، برزت ظاهرة الجريمة الإلكترونية بأنواعها المختلفة في عقد التسعينات من القرن الماضي, وارتفعت معدلاتها بشكل متسارع وأدرك المجتمع الدولي مدى الحاجة الماسة لتعاون دولي وإقليمي فعال يكبح جماح الجريمة الإلكترونية ويحد من مخاطرها الاقتصادية والاجتماعية والأمنية بعد الارتفاع الكبير في عدد مستخدمي شبكة الإنترنت حول العالم الذي كان في علم ١٩٩٣ أربعة عشرة مليون و١٦١٥٧٠مستخدم فقط وتضاعف هذا العدد في عام ٢٠١٤ إلى ٢١٣ ضعف ليصل الي أكثر من ثلاثة مليار مستخدم ، وفقا لجهاز الرصد الإلكتروني الدقيق المستمر على مدار الثانية والدقيقة والساعة ، وقد رصدنا عدد مستخدمي الانترنت حول العالم يوم ٢٠١٤/١٠/١٠ الساعة ١٤٠٥ بتوقيت عمان وكان العدد٢٩٨٦٨٠٠٠٠٠ (إثنان مليار وتسعمائة ستة وثمانون مليون وثمانمائة ألف) ,وقمنا بالرصد مرة أخرى – أثناء إعداد هذه الدراسة – في الساعة ١٩–٥ يوم ٣٠ نوفمبر ٢٠١٤ وكان العدد ٣٠١٨٦٢٧٣٥٢ (ثلاثة مليار وثمانية عشرة مليون وستمائة وسبعة وعشرون ألف وثلاثمائة واثنان وخمسون مستخدم) وتلاحظ من خلال الرصد الإلكتروني دخول ٤٢٠ مستخدم جديد كل دقيقة وبمعدل ٧ في الثانية ، ومن المؤكد أن هذا الارتفاع المذهل في أعداد المستخدمين يصاحبه ارتفاع كبير في معدلات الجريمة الإلكترونية بأنواعها المختلفة.[٩٩]

وتعد الجريمة الإلكترونية من أكثر الجرائم عبورا للحدود الوطنية transnational crime حيث أن الهجمات الإلكترونية يقوم بها شخص في دولة معينة ولكن يتأثر بها أشخاص طبيعيون أو معنيون في دول مختلفة, بل حتى أن البريد الإلكتروني email الذي يرسل إلى أشخاص في نفس الدولة من شأنه أن يشكل دليلا الكترونيا Electronic evidence في

---

٩٩ أنظر الملحق رقم (٣) للاطلاع على احصائية عدد مستخدمي الانترنت حول العالم لعام ٢٠١٤

Number of Internet Users (2014) – Internet Live Stats

وأنظر الموقع: www. Internet world states.com

مكان ما في دولة ما وقد يتم إرساله كمعلومات وبيانات إلى عدة دول، وفي نفس الوقت تأكد أن الدليل الإلكتروني سريع الزوال volatile بالطمس والاخفاء والتدمير المعتمد، ولذلك فإن التدابير المطلوبة على المستوى الوطني للحفاظ على المعلومات والبيانات المخزنة إلكترونيا ضرورية كذلك للعمل بها في إطار التعاون الدولي.

نتناول موضوعات التعاون الدولي والإقليمي لمواجهة الجريمة الإلكترونية في المطالب التالية:

المطلب الأول: اتفاقية مجلس أوربا للجريمة الإلكترونية

Council of Europe Convention on Cybercrime

المطلب الثاني: الجهود و المؤتمرات الدولية و الإقليمية لمواجهة الجريمة الإلكترونية.

المطلب الثالث: جهود التعاون الدولي لدول مجلس التعاون لدول الخليج العربية لمواجهة الجريمة الإلكترونية.

المطلب الأول

اتفاقية مجلس أوربا للجريمة الإلكترونية

Council of Europe Convention on Cybercrime

الإيجابيات وسلبيات التباطؤ في التصديق والنفاذ

وإن كان موضوع بحثنا " الجريمة الإلكترونية في المجتمع الخليجي و كيفية مواجهتها" الا أن اتفاقية مجلس أوربا [١٠٠] للجريمة الإلكترونية تعد أول مبادرة عالمية وأبرز وأنجح ثمرات التعاون الدولي في هذا المجال حتى الآن , وأنه لابد من دراسة مضمونها بشيء من التفصيل المناسب للوقوف على محاورها و استلهام و استصحاب هذه الاتفاقية الرائدة لدعم وتعزيز جهود دول مجلس التعاون لدول الخليج العربية في مكافحة الجريمة الإلكترونية بالاستفادة من تجارب و تعاون المنضمين للاتفاقية , حيث أن طبيعة الجريمة الإلكترونية أنها عابرة للحدود الوطنية وأصبحت من المهددات الأمنية العالمية بالغة الخطورة , ولابد للدول منفردة أو للتكتلات الإقليمية من دراسة تجارب المجتمع الدولي في هذا المجال لوضع الاستراتيجيات والخطط والتدابير اللازمة لمواجهة الجريمة الإلكترونية التي تستفحل بسرعة كبيرة.

أقرت اللجنة الوزارية لمجلس أوربا في دورتها رقم ١٠٩ بتاريخ ٨ نوفمبر ٢٠٠١ الاتفاقية الأوربية للجريمة الإلكترونية وتم فتح التوقيع للانضمام إلى الاتفاقية في مؤتمر دولي في بودابست – المجر – في ٢٠٠١/١١/٢٣, وفي هذا التاريخ وقعت على الاتفاقية ٢٦ دولة من الدول

---

١٠٠ توجد ثلاثة مجالس أوربية هي: ١– مجلس أوربا ٢– المجلس الأوربي ٣– مجلس الاتحاد الأوربي.
فيما يلي نبذة مختصرة توضح اختصاصات هذه المجالس والفرق بينها:
أولا: مجلس أوربا: هو منظمة دولية مكونة من ٤٧ دولة أوربية تأسست في عام ١٩٤٩ ومقر المجلس مدينة ستراسبورغ الفرنسية. العضوية في المجلس مفتوحة لكل دول أوربا الديمقراطية التي تضمن حقوق الانسان والحريات للجميع ، ومن أبرز انجازات المجلس: الميثاق الأوربي لحقوق الانسان في عام ١٩٥٠والذي بموجبه تم تأسيس المحكمة الأوربية لحقوق الإنسان. وتجدر الاشارة إلي أن مجلس أوربا لا علاقة له بالاتحاد الأوربي.
ثانيا: المجلس الأوربي: هو قمة لرؤساء الدول ورؤساء الحكومات الثمانية والعشرين الأعضاء في الاتحاد الأوربي ويعقد اجتماعين على الأقل كل سنة في شهري يوليو وديسمبر، ويختص المجلس بتعيين رئيس المفوضية الأوربية ويجري التصديق على قرار التعيين بالتصويت عليه في البرلمان الأوربي.
ثالثا: مجلس الاتحاد الأوربي: يتكون المجلس من وزراء حكومات الدول الأعضاء في الاتحاد ويشكل المجلس مع البرلمان الأوربي الذراع التشريعية للاتحاد الأوربي. للمجلس رئيس وأمين عام ، ويرأس المجلس وزير الدولة التي ترأس المجلس، ويعتبر الأمين العام الممثل الأعلى لسياسة الدفاع والخارجية المشتركة. ويجتمع المجلس أربعة مرات في العام وتعرف هذه الاجتماعات باجتماعات قمة رؤساء الاتحاد الأوربي حيث يتم في هذه الاجتماعات توجيه المجلس الأوربي ووضع سياساته العليا .

الأعضاء في مجلس أوربا Council of Europe البالغ عددها ٤٧ دولة , وعملا بالمادة (٣٧) من الاتفاقية التي تنص على انضمام الدول غير الأعضاء اليها , وقعت على الاتفاقية في ذات التاريخ أربعة دول غير أعضاء في المجلس وهي:

١. الولايات المتحدة الأمريكية.
٢. اليابان.
٣. كندا.
٤. جنوب أفريقيا.

استعراض لاتفاقية مجلس أوربا للجرائم الالكترونية لسنة ٢٠٠١:

الديباجة:

تصدرت الاتفاقية ديباجة معبرة عن رغبة الدول الأعضاء في مجلس أوربا و الدول الأخرى الموقعة على الاتفاقية عن رغبتهم و حماسهم للتعاون الدولي بشأن مكافحة الجريمة الالكترونية من خلال إقرار سياسة جنائية مشتركة تهدف إلى حماية المجتمع من الجريمة الإلكترونية وتعزيز التعاون الدولي, وإذ تدرك التغيرات العميقة التي أحدثتها الرقمية digitalization والتقارب Convergence والعولمة المستمرة لشبكات الحاسب الآلي والقلق من استخدام هذه الشبكات والمعلومات الإلكترونية لارتكاب جرائم جنائية, واعترافا بالحاجة للتعاون بين الدول والقطاع الخاص في مكافحة جرائم الإنترنت لحماية المصالح المشروعة في استخدام و تطوير تقنيات المعلومات.[١٠١]

اعتبارا لكل ما تقدم، أجاز مجلس أوربا اتفاقية الجرائم الإلكترونية وفتح التوقيع عليها للأعضاء ولغير الأعضاء في المجلس بتاريخ ٢٣/١١/ ٢٠٠١ في بودابست – المجر.

تتكون الاتفاقية من أربعة فصول كما يلي:

تناول الفصل الأول استخدام المصطلحات، ولأغراض هذه الاتفاقية تم تعريف المصطلحات التالية في المادة (١) كما يلي [١٠٢]: أ- نظام الكمبيوتر Computer System ب- بيانات

١٠١لمزيد من التفاصيل حول ديباجة الاتفاقية ، أنظر :

Convection on Cybercrime , Budapest , 23 Nov. 2001 , Council of Europe .

١٠٢ للاطلاع على التعريفات أنظر نص المادة (١) من الفصل الأول من اتفاقية مجلس أوربا للجريمة الإلكترونية .

الكمبيوتر Computer Data ج- مزود الخدمة Server Provide - د- بيانات حركة المرور Traffic data

الفصل الثاني: التدابير التي يتعين اتخاذها على المستوى الوطني:

Measures to be taken at the national level

يتكون هذا الفصل من ثلاثة أقسام: **القسم الأول**: القانون الجنائي الموضوعي Substantive Criminal Law المواد (٢-١٣) **القسم الثاني**: قانون أصول المحاكمات المواد (١٤-٢١) والقسم الثالث: الاختصاص القضائي المادة (٢٢).

الفصل الثالث: التعاون الدولي International Co-operation

اشتمل هذا الفصل على قسمين: تناول **القسم الأول** المواد (٢٣- ٣٠) المبادئ العامة المتعلقة بالتعاون الدولي ويشمل ذلك تسليم المجرمين والمساعدات المتبادلة واجراءات طلبات المساعدات المتبادلة في غياب الاتفاقيات الدولية الواجبة التطبيق. واختص **القسم الثاني** في المواد (٣١-٣٥) بالمساعدات المتبادلة بشان التدابير المؤقتة والمساعدات المتبادلة فيما يتعلق بسلطات التحقيق ومكافحة استخدام شبكة الإنترنت لارتكاب الجرائم الإلكترونية.

الفصل الرابع: نصت الاتفاقية علي الأحكام الختامية في المواد (٣٦-٤٨) وتعد المادة (٣٧): الانضمام للاتفاقية من أبرز ما ورد في الأحكام الختامية، وقد نصت الفقرة (١) على أن: (الاتفاقية مفتوحة للتوقيع عليها من الدول غير الاعضاء بمجلس اوروبا التي لم تشارك إعدادها وإجازتها). وتنص الفقرات ٢، ٣، ٤ على شروط انضمام الدول غير الأعضاء للاتفاقية.[١٠٣]

البروتوكول الاضافي لاتفاقية مجلس اوروبا للجريمة الإلكترونية:

صدر هذا البروتوكول في ستراسبورغ – فرنسا - في ٢٨ نوفمبر ٢٠٠٣ واشتمل على أربعة فصول جاء **الفصل الأول** بعنوان: الأحكام العامة (المواد ١، ٢) - **الفصل الثاني**: بشأن التدابير التي يجب اتخاذها على المستوى الوطني (المواد ٣-٧) - **الفصل الثالث**: حول العلاقة بين الاتفاقية والبروتوكول (المادة ٨) أما **الفصل الرابع**: عن الأحكام الختامية في المواد (٩-١٦).

١٠٣ أنظر المذكرة الاخبارية حول مشاركة الدول غير الأعضاء في مجلس أوربا في معاهدات المجلس .

الأهداف الاساسية لاتفاقية مجلس أوربا للجريمة الالكترونية [١٠٤]:

١- تحقيق التوافق والانسجام بين عناصر الجرائم في القوانين الجنائية المحلية الأساسية, والشروط المتطلبة ذات الصلة في مجال الجريمة الإلكترونية.

٢- تزويد قوانين الاجراءات الجنائية المحلية – في دول الاتحاد الأوربي و غيرها – بصلاحيات ضرورية للتحقيق وتوجيه الاتهام في الجرائم الإلكترونية وغيرها من الجرائم التي ترتكب باستخدام أنظمة الحاسب الآلي والتعامل مع الأدلة ذات العلاقة بالطابع الإلكتروني.

٣- إعداد نظام فعال وسريع للتعاون الدولي.

إحصائية موقف الدول من التوقيع والتصديق والانفاذ لاتفاقية مجلس أوربا للجريمة الإلكترونية:

في آخر إحصائية بتاريخ ٢٠١٤/١٠/٥ عن موقف الدول من التوقيع على الاتفاقية و التصديق عليها و دخولها حيز النفاذ, وقعت بقية الدول الأعضاء في مجلس أوربا الـ ٢٩ على الانضمام للاتفاقية في تواريخ متفاوتة بعد ٢٣ /٢٠٠١/١١ ويلاحظ أن الحماس للتوقيع لم يكن بالقدر المطلوب الذي ورد في ديباجة الاتفاقية حيث وقعت آخر دولتين أعضاء في مجلس أوربا في عام ٢٠١٣ وهما موناكو في ٢٠١٣/٢/٢٥ واندروا Andorra في ٢٠١٣/٤/٢٣ وحتى تاريخ هذه الاحصائية لم توقع على الاتفاقية دولتان هما روسيا وسان مارينو San Marino أما الدول غير الأعضاء التي انضمت إلى الاتفاقية حتى تاريخ ٢٠١٤/١٠/٥ بلغ عددها ١٣ دولة إضافة إلى الأربعة دول السالفة الذكر التي وقعت عند فتح الاتفاقية للتوقيع بتاريخ ٢٠٠١/١١/٢٣.[١٠٥]

تحليل موقف الدول الموقعة على الاتفاقية:

تأخرت الدول الأوربية الغربية الأعضاء في مجلس أوربا كثيرا في التصديق على الاتفاقية Ratification , علما بأن تسعة من دول أوربا الشرقية بالإضافة إلى مالطا هي الأسبق في التصديق على الاتفاقية خلال الفترة من ٢٠٠٢/٦/٢٠ إلى ٢٠٠٥/٥/١ وهي: استونيا

١٠٤ أنظر المذكرة التفسيرية لاتفاقية مجلس أوربا للجريمة الإلكترونية:

Council of Europe- Explanatory Report to the Convection on Cybercrime , (ETS No.185) Introduction, No. 111, The Convection , p.3.

١٠٥ أنظر إحصائية موقف التوقيع والتصديق والنفاذ لاتفاقية مجلس أوربا للجريمة الإلكترونية حتى ١٠/٥ / ٢٠١٤، ملحق رقم (٧) ص أ–د

– هنغاريا – ليتوانيا – رومانيا – سلوفينيا – ماكدونيا – بلغاريا – مالطا, والخمسة الأوائل من هذه الدول التزمت بإدخال الاتفاقية حيز النفاذ في التاريخ المحدد في الاتفاقية وهو ٢٠٠٤/٧/١ ودخلت الاتفاقية حيز النفاذ في سلوفينيا وماكدونيا في ٢٠٠٥/١/١.

مما تقدم يتضح كذلك عدم حماس الدول الغربية الصناعية الكبرى المتقدمة تكنولوجيا للتصديق على الاتفاقية وإدخالها حيز النفاذ في الوقت المحدد بعد التوقيع عليها كما فعلت دول أوربا الشرقية, ومثال ذلك أنظر الجدول أدناه:

البلد	التوقيع	التصديق	النفاذ
فرنسا	23/11/2001	10/1/2006	1/5/2006
ألمانيا	23/11/2001	9/3/2009	1/7/2009
إيطاليا	23/11/2001	5/6/2008	1/10/2008
المملكة المتحدة	23/11/2001	25/5/2011	1/9/2011

وقد كشف تحليل[١٠٦] إحصائية التوقيع والتصديق والنفاذ لاتفاقية مجلس أوربا للجريمة الإلكترونية أن ١٠ دول أعضاء بنسبة ٢٣,٢٥٪ قد وقعت على الاتفاقية في الفترة من ٢٠٠٤ إلى ٢٠٠٥ وأن ١٣ دولة بنسبة ٣٠,٤٪ صدقت على الاتفاقية وأدخلتها حيز النفاذ في الفترة من ٢٠٠٦ إلى ٢٠٠٩ أما الدول الأعضاء التي صدقت على الاتفاقية وأدخلتها حيز النفاذ في الفترة من ٢٠١٠ إلى ٢٠١٤ بلغ عددها ١٣ دولة بنسبة ٣٠,٤ ٪ .

أما الدول الأربعة غير الأعضاء في مجلس أوربا التي بادرت بالتوقيع على الاتفاقية في مؤتمر بودابست بتاريخ ٢٠٠١/١١/٢٣، فهي الأخرى لم يكن حماسها للتصديق على الاتفاقية وادخالها حيز النفاذ بالمستوى المطلوب، وفيما يلي موقف هذه الدول الذي يؤكد ما ذهبنا اليه:

الدولة	التوقيع	التصديق	النفاذ
الولايات المتحدة الأمريكية	23/11/2001	29/9/2006	1/7/2006
اليابان	23/11/2001	3/7/2012	1/11/2012
كندا	23/11/2001	30/11/2012	1/3/2013
جنوب أفريقيا	23/11/2001	لم تصدق حتى الآن	ـــــ

١٠٦ قام بتحليل الاحصائيات فريق البحث بمجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة.

أما استراليا فقد صدقت على الاتفاقية في ٣٠/١١/ ٢٠١٢ وأدخلتها حيز النفاذ في ١/٣/ ٢٠١٣.

قصدنا بهذا التحليل لموقف الدول الاعضاء في مجلس أوربا Council of Europe من اتفاقية الجريمة الإلكترونية أن نسلط الضوء على مدى التباطؤ المقصود من غالبية الدول في التصديق على الاتفاقية وانفاذها حيث أن ٣٠٪ من الأعضاء صدقوا عليها و نفذوها بعد مرور ٥ إلى ٨ سنوات من فتحها للتوقيع وأن ٣٠٪ أخرى من الاعضاء صدقوا عليها وأدخلوها حيز النفاذ بعد مرور٩ إلى ١٣ سنة من فتحها للتوقيع في ٢٣/١١/٢٠٠١ , أي أن ٦٠٪ من الأعضاء الموقعين على الاتفاقية أدخلوها حيز النفاذ بعد فترة تراوحت بين ٥ سنوات إلى ١٣ سنة. مما يؤكد أن التوقيع على الاتفاقية كان بالنسبة لبعض الدول عبارة عن تظاهرة دوليه للعلاقات العامة أعقبها تقاعس متعمد في التصديق عليها وانفاذها.

وعلى الرغم من أن الاتفاقية تعد رائدة في مجالها وتعد نموذجا يصلح لتعاون دولي في مواجهة الجريمة الإلكترونية Global Cooperation on Cybercrime إلا أن عدم التصديق على الاتفاقية وإدخالها حيز النفاذ في أقرب وقت ممكن أدى إلى تعطيل فعلي لهذا التعاون الدولي المنشود لفترة تصل إلى عشرة سنوات تقريبا وهي الفترة التي استفحلت فيها الجريمة الإلكترونية بكل أنواعها وأدت إلى خسائر مادية كبيرة جدا على نطاق العالم بما في ذلك منطقة الخليج العربي، حيث وصلت الخسائر العالمية في عام ٢٠١٣ إلى أكثر من ٤٥٠ مليار دولار[١٠٧] وتهديدات بخسائر أكبر, وجاءت الانتباهة لهذا الخطر الداهم متأخرة جدا بعد عام ٢٠١٠, وفي رأينا أن أعضاء اتفاقية دول مجلس أوربا للجريمة الاليكترونية، إضافة إلى الدول الأخرى المؤثرة الأعضاء في الاتفاقية من غير الأعضاء في مجلس أوربا كالولايات المتحدة الأمريكية وكندا واليابان واستراليا، قد أسهمت كل هذه الدول في تعطيل تفعيل هذه الاتفاقية الهامة بوصفها أول وأهم مبادرة عالمية للتعاون الدولي لمواجهة الجريمة الاليكترونية، حيث أن التحرك الدولي المكثف لتفعيل الاتفاقية بدأ أكثر حماسا وفاعلية اعتبارا من عام ٢٠١٠ بعد أن طالت الهجمات البنيات التحتية وبلغت الخسائر مئات المليارات من الدولارات ولازالت التهديدات مستمرة بهجمات تسبب أضرار جسيمة للبنيات التحتية في القطاع العام والخاص ومعلومات وبيانات الأفراد وتخلف آثاراً سلبية على الاقتصاد العالمي والأعوام التالية، ولذلك يفترض أن تتحمل هذه الدول تداعيات التباطؤ المتعمد في التصديق على اتفاقية مجلس أوربا الجريمة الإلكترونية وانفاذها ومواجهة المخاطر والتهديدات في الوقت المناسب.

---

١٠٧ أنظر المرجع التالي: Cyber Crime Statistics and Trends. 2014 Report. www.go.gulf.com

المطلب الثاني
الجهود والمؤتمرات الدولية والاقليمية
لمواجهة الجريمة الاليكترونية

مقدمة:

تكمن أهمية الجهود الدولية والاقليمية لمواجهة الجريمة الإلكترونية في أنها وضعت الأساس الذي تم بموجبه توقيع اتفاقية مجلس أوربا للجريمة الإلكترونية في ٢٠٠١/١١/٢٣ Council of Europe convection on Cybercrime بوصفها أول مبادرة دولية في هذا الشأن, وتواصلت هذه الجهود في مؤتمر الامم المتحدة العاشر لمنع الجريمة والعدالة الجنائية عام ٢٠٠٥والمؤتمر الثاني عشر عام ٢٠١٠ الذي أدرج ''جرائم الانترنت '' في جدول أعماله لأول مرة في تاريخ مؤتمرات الأمم المتحدة لمنع الجريمة والعدالة الجنائية منذ انعقاد أول اجتماع لها في جنيف عام ١٩٥٥م. وتواصلت الجهود في مؤتمرات قمة دول مجموعة الثمانية G-8[١٠٨], وغيرها من المؤتمرات واللقاءات الدولية والإقليمية التي تهدف لإرساء قواعد قوية لبناء استراتيجية عالمية فعالة لمكافحة الجريمة الاليكترونية ,ولذلك لا غنى لدول مجلس التعاون الخليجي العربية وغيرها من دول العالم غير الأوربية من استصحاب الجهود الدولية في هذا المجال واستيعابها والاستفادة من التجارب والخبرات العالمية ولاستخلاص طرق منهجية لإعداد استراتيجية محكمة وفعالة ترسم خارطة الطريق لمكافحة الجريمة الإلكترونية.

ونظراً لكثافة الجهود الدولية في مكافحة الجريمة الإلكترونية، نستعرض بإيجاز أهم النماذج لهذه الجهود على سبيل المثال وليس الحصر:

خلفية تاريخية لجهود مجموعة الدول الثمانية G-8 لمكافحة الجريمة الإلكترونية:

عام ١٩٩٧: أنشأت مجموعة الدول الثمانية G-8 فريق فرعي للجرائم الإلكترونية الفائقة التقنية.

---

١٠٨ مجموعة الدول الثمانية G-8 أو مجموعة الدول الصناعية الثمانية الكبرى في العالم وتضم الولايات المتحدة الأمريكية – اليابان – المانيا – روسيا الاتحادية – ايطاليا – المملكة المتحدة فرنسا وكندا, يمثل مجموع اقتصاد هذه الدول الثمانية ٦٥٪ من اقتصاد العالم وأغلبية القوة العسكرية حيث تمثل هذه الدول ٧ من ٨ مراكز الأكثر اتفاقاً على التسلح في العالم , وتتضمن أنشطة المجموعة مؤتمرات على مدار السنة وقمة سنوية للدول الأعضاء ويتم تمثيل الاتحاد الأوربي في القمة السنوية برئيس الدولة الأوربية التي تتولى الرئاسة الدورية للاتحاد الأوربي.

وتجدر الاشارة إلى أن هذه المجموعة أنشأتها الولايات المتحدة الأمريكية لأول مرة سنة ١٩٧٤بعد الأزمة النفطية عام ١٩٧٢وماتبعها من ركود اقتصادي أدى لتبلور مفهوم تجمع الدول الصناعية الكبرى فتكونت المجموعة لأول مرة من خمسة دول هي: الولايات المتحدة الأمريكية والمملكة المتحدة وألمانيا الغربية واليابان وفرنسا و انضمت إيطاليا في اجتماع قمة ١٩٧٥م وانضمت كندا في قمة ١٩٧٧ وعرفت وقتها بمجموعة السبعة وفي عام ١٩٩٧ تمت دعوة روسيا للانضمام وصارت تدعى مجموعة الثمانية (G8).

وفي اجتماع عقد في واشنطن عام The G-8 Subgroup High-Tech Crime ١٩٩٧اعتمدت مجموعة الدول الثمانية G-8عشرة مبادى لمكافحة جرائم الحاسوب, وكان الهدف ألا يحصل المجرم على ملذات آمنة في أي مكان في العالم .

قمة مجموعة G-٨ في ١٠ /٢٠٠٤/١١م:

في اجتماع قمة مجموعة الدول الثمانية G-8 الذي ضم وزراء العدل والداخلية في واشنطن في ٢٠٠٤/١١/١٠م , صدر بيان مشترك تضمن ما يلي:

" مواصلة تعزيز القوانين المحلية لبناء القدرات العالمية لمكافحة الاستخدامات الإرهابية والإجرامية للإنترنت, ويجب على جميع الدول أن تواصل تحسين القوانين التي تجرم إساءة استخدام الشبكات الحاسوبية والتي تسمح بسرعة التعاون في التحقيقات المتصلة بالإنترنت, ومع دخول اتفاقية مجلس أوربا للجريمة الإلكترونية حيز النفاذ في ٢٠٠٤/٧/١, يجب علينا - يقصد البيان الدول الأعضاء في الاتفاقية- اتخاذ خطوات لتشجيع اعتماد المعايير القانونية التي تتضمنها على قاعدة واسعة "[١٠٩].

بيان مجموعة G-8عام ٢٠٠٥:

في بيان صادر عن اجتماع مجموعة دول G-8 في عام ٢٠٠٥ تم التأكيد على الهدف وهو: "التأكيد على أن وكالات إنفاذ القانون تستجيب بسرعة لتهديدات الجريمة الإلكترونية والحوادث الخطيرة" .[١١٠]

اجتماع مجموعة G-8 – موسكو عام ٢٠٠٦:

وفي اجتماع موسكو في عام ٢٠٠٦ لوزراء العدل والداخلية لدول مجموعة الثمانية G-8 ، تمت مناقشة الجريمة الإلكترونية وقضايا الفضاء الإلكتروني "Cyberspace" وصدر بيان موسكو الذي تم فيه التأكيد على الآتي:

".... أنه من الضروري اتخاذ مجموعة من التدابير لمنع الأعمال الاجرامية المحتملة, بما في ذلك مجال الاتصالات السلكية واللاسلكية والعمل ضد بيع البيانات الخاصة والمعلومات المزيفة وتطبيقات الفيروسات وبرامج الكمبيوتر الضارة الأخرى, سنوجه خبراءنا لتعميم مناهج موحدة

---

١٠٩ نظر مركز معلومات G-8على الموقع الاليكتروني : http://www.CybercimeLaw.net/G8.html

١١٠ أنظر الموقع الاليكتروني السابق.

لمكافحة الجريمة الإلكترونية , وسوف نحتاج للقواعد القانونية الدولية لهذا العمل, وسوف نطبق كل ذلك لمنع الارهابيين من استخدام مواقع الكمبيوتر والإنترنت لتوظيف الارهابيين الجدد وتوظيف الجهات الفاعلة غير القانونية الأخرى.(١١١)

اجتماع قمة دول الثمانية G-8 في سانت بطرسبرغ عام ٢٠٠٦:

صدر إعلان القمة بشأن مكافحة الإرهاب وتضمن ما يلي: "نؤكد من جديد التزامنا بالتعاون مع شركائنا الدوليين لمكافحة التهديد الإرهابي بما في ذلك:

- تنفيذ وتحسين الاطار القانوني الدولي لمكافحة الإرهاب.
- التصدي بفاعليه لمحاولات اساءة استخدام الفضاء الإلكتروني misuse cyberspace لأغراض إرهابية بما في ذلك التحريض على ارتكاب أعمال إرهابية, وعلى التواصل مع الإرهابيين وصنع الخطط الإرهابية وتجنيد وتهريب الإرهابيين "(١١٢)

اجتماع وزراء العدل والداخلية لدول مجموعة الثمانية G-8 في ٢٣-٢٥مايو - ميونخ - المانيا - ٢٠٠٧:

أتفق الأعضاء على: " العمل من خلال الاطر القانونية الوطنية national legal frameworks لتجريم أشكال معينة بشأن استخدام الإنترنت لأغراض إرهابية ".(١١٣)

قمة G-8 في ايطاليا عام ٢٠٠٩م:

وبالتزامن مع هذه القمة التقى وزراء العدل والداخلية في روما في ٢٨-٣٠مايو ٢٠٠٩ وأصدرت القمة بيانا تضمن جرائم الإنترنت والأمن السيبراني وإشارت إلى تقرير صدر عن مجموعة روما/ ليون قدم لمفوضية الأمم المتحدة لمنع الجريمة والعدالة الجنائية – وأشار البيان إلى أن التقدم التكنولوجي أسفر عن " إساءة استعمال الشبكات الاجتماعية Social Networks وخدمات التشفير Encryption Services وخدمات النطاقات The Domain Name System, وأن الهجمات الإجرامية الجديدة المتطورة الأخرى Criminal attacks على أنظمة المعلومات تشكل تحديات إضافية تواجه انقاذ القانون ".

---

١١١ أنظر الموقع الاليكتروني السابق : G-8 Information Center

١١٢ أنظر الموقع الاليكتروني السابق.

١١٣ أنظر الموقع السابق لمفوضية الأمم المتحدة لمنع الجريمة والعدالة الجنائية: UN Commission on Crime Prevention and Criminal Justice

قمة دول G-8 في دوفيل فرنسا ٢٠١١:

صدر إعلان قمة G-8 في دوفيل فرنسا في ٢٦ مايو ٢٠١١ واختص الجزء الثاني من الاعلان بقضايا الإنترنت في البنود من ٤ الى ٢٢ وأكد الإعلان على أن شبكة الإنترنت أصبحت ضرورية في كافة انحاء العالم لمجتمعاتنا واقتصادياتها ونموها, وهي مصدر فريد للمعلومات والتعليم للمواطنين ولتعزيز الحرية والديمقراطية وحقوق الانسان , كما أن شبكة الإنترنت أصبحت أداة أساسية لتسيير التجارة ولتطوير العلاقات مع المستهلك, كما أنها بالنسبة للحكومات أداة للإدارة أكثر كفاءة وتعد الشبكة محركاً رئيسياً للاقتصاد العالمي والنمو والابتكار والانفتاح والشفافية.

وأكد إعلان دوفيل على أهمية الاقتصاد الرقمي العالمي The Global Digital Economy كمحرك اقتصادي قوى ومحرك للنمو والابتكار, وتناول الاعلان حماية الملكية الفكر به وحماية البيانات الشخصية والخصوصية وأمن الشبكات ومكافحة اساءة استخدام الإنترنت للإتجار في الأطفال والأغراض الأخرى غير المشروعة، والتشجيع لاستخدام الإنترنت لأغراض التنمية لاسيما التعليم والرعاية الصحية في البلدان النامية, ودعا الاعلان إلى تعزيز التعاون داخل وبين جميع المحافل الدولية التي تتناول حركة الإنترنت.[١١٤]

مؤتمرات الجريمة الإلكترونية الدولية والإقليمية:

بعد أن ارتفعت معدلات ارتكاب الجرائم الإلكترونية بشكل ملحوظ ومتسارع على نطاق العالم في الخمس سنوات الأخيرة ٢٠٠٩ إلى ٢٠١٤- ولما كانت غالبية الأضرار والتهديدات تقع على كاهل الدول المتقدمة اقتصاديا وتكنولوجيا, مرة أخرى انتبه المجتمع الدولي لضرورة اتخاذ كل التدابير اللازمة لتفعيل اتفاقية مجلس أوربا للجريمة الإلكترونية Council of Europe Convention on Cybercrimeمن أجل تحقيق أهدافها في مكافحة الجريمة الإلكترونية ,وبالإضافة إلى مؤتمرات واجتماعات دول مجموعة الثمانية G-8 التي أشرنا إليها, عقدت في الفترة الأخيرة منذ عام ٢٠١٠وحتى هذا العام ٢٠١٤عشرات المؤتمرات وورش العمل والسمنارات في شأن مواجهة الجريمة الإلكترونية, ونظراً لتحديد حيز البحث، سنكتفي بالإشارة الى مؤتمرات الأمم المتحدة وهي محدودة جداً في هذا الشأن وبعض المؤتمرات الأخرى التي عقدت عام ٢٠١٤ فقط لتأكيد مدى كثافة هذا الحراك الدولي لمكافحة الجريمة الإلكترونية.

---

١١٤ أنظر إعلان قمة دول G-8 في دوفيل – فرنسا، ٢٦ مايو ٢٠١١, G-8information Centre ,Deauville Declaration

http://www.g8.utoronto.ca/summit/2011/deaurille/2011-lmternet-en-html

مؤتمرات الأمم المتحدة لمنع الجريمة والعدالة الجنائية:

عقدت الأمم المتحدة حتى الان ١٢مؤتمرا دولياً لمنع الجريمة ومعاملة المجرمين وكان المؤتمر الأول قد عقد في جنيف عام ١٩٥٥, غير أن موضوع الجريمة الإلكترونية ناقشته الأمم المتحدة لأول مرة في مؤتمر الأمم المتحدة العاشر لمنع الجريمة والعدالة الجنائية عام ٢٠٠٠.

عقد مؤتمر الامم المتحدة العاشر لمنع الجريمة والعدالة الجنائية لعام ٢٠٠٠ في فيينا- النمسا من ١٥ إلى ١٧ أبريل ٢٠٠٠ وحضر المؤتمر ممثلو ١١٩ دولة منهم ٧٦ وزيراً ومسؤولاً رفيع المستوى , ومن أبرز الموضوعات التي ناقشها المؤتمر التعاون الدولي في مكافحة الجريمة المنظمة عبر الوطنية ''التحديات الجديدة في القرن الحادي والعشرين وصدر إعلان المؤتمر وهو يتضمن لأول مرة: ''تأكيدا للحاجة إلى التصدي للموجة المتزايدة من الجرائم الحاسوبية ..'' [١١٥]

مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية عام ٢٠١٠:

عقد هذا المؤتمر في سلفادور- البرازيل من ١٢-١٩أبريل ٢٠١٠ تحت عنوان: استراتيجيات شاملة لتحديات عالمية: ''نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير '' وتضمن جدول أعمال المؤتمر ثمانية بنود كان من بينها: ''جرائم الإنترنت أو الشبكة العنكبوتية'' والتعاون الدولي في مكافحة الجريمة.

لجنة منع الجريمة والعدالة الجنائية[١١٦] للأمم المتحدة تتابع جدول أعمال مؤتمر الأمم المتحدة لمنع الجريمة عام ٢٠١٥ الذي يتضمن الجريمة المنظمة العابرة للحدود الوطنية:

عقدت اللجنة دورتها الثانية والعشرين في فيينا ٢٢-٢٦ إبريل ٢٠١٣وكان البند (٨) من جدول الأعمال: متابعة نتائج مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية والاعمال التحضيرية للمؤتمر الثالث عشر الذى سيعقد عام ٢٠١٥ والذي يضمن جدول أعماله: التعاون الدولي, بما ذلك التعاون على الصعيد الاقليمي لمكافحة الجريمة المنظمة العابرة للحدود الوطنية.

كما أصدرت الجمعية العامة للأمم المتحدة القرار ١٨٤/٦٧ بتاريخ ٢٠ ديسمبر ٢٠١٢الذي أجاز جدول الأعمال لمؤتمر الامم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية المقرر عقدة في الدوحة في الفترة من: ١٢ إلى ١٩ إبريل ٢٠١٥ تحت شعار «إدماج منع الجريمة والعدالة

---

١١٥ أنظر وثائق المؤتمر في الموقع الإلكتروني لمفوضية الأمم المتحدة لمنع الجريمة والعدالة الجنائية.

١١٦ هذه اللجنة تابعة للأمم المتحدة.

الجنائية في جدول أعمال الأمم المتحدة الاوسع من أجل التصدي للتحديات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطني والدولي ومشاركة الجمهور», وقررت اللجنة عقد ورشة عمل في إطار المؤتمر الثالث عشر القادم بشأن « تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة مثل الجريمة السيبرانية والاتجار بالممتلكات الثقافية, بما في ذلك الدروس المستفادة والتعاون الدولي.

مؤتمر قمة الأمن السيبراني - مملكة البحرين ٢٠ -٢٢أكتوبر ٢٠٠١٤:

ناقشت هذه القمة الموضوعات التالية:

- بحث سبل إعادة الأمن واستراتيجية تكنولوجيا المعلومات.
- إعادة تعريف المخاطر.
- تنفيذ أفضل الممارسات لتحقيق مدونه التهديدات.
- تخفيف مخاطر أدوات التواصل الاجتماعي الجديدة.
- استراتيجية مواجهة التهديدات المتنقلة.
- الاستغلال الجنسي للأطفال[١١٧].

مؤتمر قمة الأمن السيبراني مينابولس, مينيسوتا, الولايات المتحدة الامريكية ٢١-٢٢اكتوبر ٢٠١٤:

شارك المؤتمر ممثلين من القطاعين العام والخاص لمناقشة التدابير المضادة للتهديدات الإلكترونية [١١٨], وتعزيز أمن القطاع العام والخاص في مواجهة الجريمة الإلكترونية وقياس مدى تأمين برامج الحاسب الآلي ضد الهجمات وتطوير تحقيقات الشرطة ومهارات التحقيق التقنية والأدلة العلمية والاستراتيجيات الشاملة لمواجهة الجريمة الإلكترونية [١١٩].

مؤتمر الانتربول واليورو بول الثاني للجريمة الاليكترونية سنغافورة ١-٣ أكتوبر ٢٠١٤:

INTERPOL/EUROPOL Cybercrime Conference 2014 1-3 October 2014

دعمت عقد هذا المؤتمر أحد الجهات الاعتبارية الدولية الفاعلة في مكافحة الجريمة الاليكترونية

---

١١٧ CSEC 2014 Cyber security Summit, Kingdom of Bahrain, October 20-22,2014

١١٨ Cyber Security Summit 2014,Minneapolis,Minnesta, USA .October 21-22,2014.

١١٩ أنظر ورقة العمل التالية التي قدمت لمؤتمر قمة الأمن السيبراني في مينيسوتا المشار اليه:
Developing Police Force Cybercrime investigation Skills and Techniques-Digital Forensics Technology and Comprehensive Cybercrime Strategies.

وتعرف بـ ''الجهود الدولية في الجريمة الإلكترونية '' وتسمى اختصارا''GLACy''[١٢٠] وقد أسهمت بدعمها بتمكين خبراء في الجريمة الإلكترونية من أكثر عشرين دولة من المشاركة في المؤتمر الذي يهدف إلى تسهيل مهمة الوحدات المتخصصة في مكافحة الجريمة الإلكترونية في الاتصال بين بعضها البعض من خلال الشبكة الدولية International Networking.

عقد المؤتمر تحت شعار ''**تحقيقات الجرائم الإلكترونية دورة كاملة** ''وشارك فيه ممثلون لسلطات انفاذ القانون والقطاع الخاص والأوساط الاكاديمية والمنظمات الدولية من مختلف أنحاء العالم , وناقش المؤتمر ''تحقيقات الجرائم الاليكترونية وأحدث التقنيات المستهدفة من هذه التحقيقات بهدف تعزيز التعاون في مجالات الجريمة الإلكترونية التالية:

- الوقاية والكشف.
- التحقيق، تقنيات التعقب والمصادرة والطلب الشرعي.
- الملاحقة والمحاكمة.

مؤتمر الأمن السيبراني/ جامعة نيويورك للتكنولوجيا ١٨سبتمبر ٢٠١٤:

شارك في هذا المؤتمر خبراء الانترنت والشركات والحكومات وناقش المؤتمر الموضوعات التالية:

- الخصوصية – الابتكارات في المؤسسة الاجنبية – أنظمة الأمن والإنترنت حماية البنية التحتية الحساسة والمنظمات والأفراد من الهجمات الإلكترونية[١٢١].

مؤتمر (GLACY) لبناء القدرات في بور لويس عاصمة جزر موريشيوس ١١-١٤أغسطس٢٠١٤:

GLACY :Capacity Building in Mauritius – Conference and workshops

عقد هذا المؤتمر تحت رعاية ''الجهود الدولية في الجريمة الإلكترونية GLACY'' وقام مجلس أوربا للجريمة الإلكترونية بدعم سلسله من نشاطات بناء القدرات في الفترة من ١١–١٤ أغسطس ٢٠١٤وناقشت ورش العمل والمؤتمر الموضوعات التالية:

- اتفاقية مجلس أوربا للجريمة الإلكترونية.

---

١٢٠ «G l AC Y" اختصار للاسم التالي : Global Action on Cybercrime وهي مشروع مشترك لمكافحة الجريمة الاليكترونية بين الاتحاد الاوربي European Union ومجلس أوربا Council of Europe كذلك يشارك في المشروع ''مركز اليورو بول لمكافحة الجريمة الاليكترونية Europol. The European Cybercrime Centre Ec3 at وتستضيف الانتربول المؤتمر في مجمعها العالمي في سنغافورة .

١٢١ Cyber security Conference, New York University Technology,18sept-2014.

- مدى إمكانية حصول سلطات انفاذ القانون على المعلومات.[١٢٢]

(Law enforcement access to data)

- استراتيجيات تدريب منسوبي سلطات انفاذ القانون ومنسوبي السلطات القضائية.
- حماية الطفل.
- إعادة النظر في القانون الجنائي لمواكبة مقتضيات مكافحة الجريمة الإلكترونية.
- التعاون الدولي.

ورشة عمل دولية حول التدريب القضائي بشأن الجريمة الإلكترونية والأدلة الإلكترونية في بوخاريست-رومانيا ٢-٣ يونيو٢٠١٤:[١٢٣]

تم عقد هذه الورشة تحت رعاية «الجهود الدولية في الجريمة الإلكترونية «GLACY'' بالمشاركة مع مجموعة الدول الاوربية الشرقية , وقد تبنى مجلس أوربا Council of Europe مفهوماً لتدريب القضاة وأعضاء الادعاء العام في مجال الجريمة الإلكترونية, وتم اختبار هذا المفهوم في جنوب شرق أوربا وقد جرى تطوير عدد من مواد التدريب وذلك بعقد دورات أساسية Basic Coursesوأخرى متقدمة Advanced Courses ودورات في الأدلة الإلكترونية Electronic Evidence Guide وكان الهدف من ورشة العمل دعم تأصيل هذا المفهوم في دورات تدريب القضاة المحلية في الدول المستفيدة من التدريب تحت رعاية شراكة دول شرق أوربا لمكافحة الجريمة الإلكترونية

EU/COE EASTERN PARTNERSHIP FACILITY المعروفة اختصارا ب(EAP) وكذلك دعم الجهود الدولية في الجريمة الإلكترونية GLACY''

١٢٢ عقدت (GLACY) مؤتمرا خاصاً في مقر مجلس أوربا في استراسبورغ في ١٩ -٢٠ يونيو٢٠١٤ وقد تم عقد هذا المؤتمر بدعم اليابان المتواصل لنشاطات مجلس أوربا لمكافحة الجريمة الإليكترونية ومنها '' مشروع الأخطبوط لمكافحة الجريمة الاليكترونية (Project Cybercrime @ Octopus) ''ويهدف المؤتمر لمناقشة ضمانات المادة (١٥) من اتفاقية مجلس أوربا للجريمة الإلكترونية لشأن تمكين سلطات انفاذ القانون من المعلومات, وقد كان المؤتمر مفتوحاً لمشاركة ممثلي منظمات المجتمع المدني ومقدمي خدمات الانترنت والصحافة الاجتماعية.

١٢٣ GLACY/Cyber crime @EAP:/International Workshop on mainstreaming judicial training on Cybercrime and electronic evidence, Bucharest,Romania,2-3June 2014.

ورشة عمل دولية في استراتيجيات تدريب أعضاء سلطات تنفيذ القانون والحصول على مواد التدريب "لاهاي- هولندا ١٢- ١٦مايو ٢٠١٤:

GLACY Cybercrime @EAP: International Workshop on Law Enforcement Training Strategies and Access to Training Materials. The Hague, Netherlands 12-16 May 2014

كانت هذه الورشة مخصصة لممثلي معاهد التدريب التابعة لأجهزة الادعاء العام المختصة في مكافحة الجريمة الإلكترونية, إضافة إلى ممثلي وحدات مكافحة الجريمة الاليكترونية Cybercrime Units, وهدفت الورشة إلى تطوير الاستراتيجيات المحلية لتدريب منسوبي سلطات انفاذ القانون وتمكينهم من الحصول على مواد التدريب التي تم تطويرها بواسطة " المجموعة الأوربية للجريمة الإلكترونية للتدريب والتعليم "[١٢٤]

ورشة عمل دولية في تشريعات الجريمة الإلكترونية مكسيكيو سيتي ٢١مارس -٢ أبريل ٢٠١٤:

نظمت الحكومة المكسيكية ورشة العمل بالتعاون مع مجلس أوربا للجريمة الإلكترونية، وتهدف إلى استقطاب دول أمريكا اللاتينية للانضمام إلى اتفاقية المجلس الأوربي لمكافحة الجريمة الإلكترونية , شارك في الورشة ٢٠٠من ممثلي السلطات القضائية والادعاء العام والسلطات التنفيذية وممثلي القطاع الخاص من المكسيك بالإضافة إلى ممثلين من الارجنتين, شيلي, كولمبيا , كوستاريكا, دومينكان, بنما, بروجوى، وبيرو.

ورشة عمل تشريعات الجريمة الإلكترونية في غرب إفريقيا أكرا /غانا ١٨-٢١مارس ٢٠١٤:

عقدت هذه الورشة بدعم من مجلس أوربا للجريمة الإلكترونية بهدف تحقيق الموازنة والانسجام بين تشريعات غرب أفريقيا بشأن مكافحة الجريمة الاليكترونية وقد استضاف الورشة «مركز كوفي عنان الدولي للتدريب على حفظ السلام « [١٢٥] في أكرا – غانا .

مؤتمر الجهود الدولية لمكافحة الجريمة الإلكترونية GLACY في داكار - السنغال ٢٤-٢٧مارس ٢٠١٤:

عقد المؤتمر بدعم مجلس أوربا للجريمة الإلكترونية وبمشاركة الاتحاد الاوربي وأكثر من ١٠٠ ممثل وخبراء الجريمة الإلكترونية عن أكثر من ٣٠ دولة .[١٢٦]

١٢٤ European Cybercrime Training and Education Group (ECTEG)

١٢٥ Coif Annan International Peace Keeping Training Centre in Accra, Ghana, from 18 to 21 March2014.

١٢٦ GLACY Conference : Getting started ,24-27March 2014 Dakar , Senegal

المطلب الثالث

جهود التعاون الدولي والإقليمي لدول مجلس التعاون لدول الخليج العربية لمواجهة الجريمة الإلكترونية خلال هذا عام ٢٠١٤

تكثفت هذه الجهود في العام ٢٠١٤ وبرزت في شكل مؤتمرات لطرح ومناقشة قضايا الأمن السيبراني ونذكر فيما يلى بعضها على سبيل المثال لتأكيد اهتمام هذه الدول بمواجهة الجريمة الإلكترونية ومواكبتها للجهود الدولية في هذا المجال.

مؤتمر أبوظبي العالمي للأمن السيبراني[١٢٧] التهديدات الوطنية والمشتركة - الحماية والتعليم ٢٥مارس ٢٠١٤:

تم عقد هذا المؤتمر بمشاركة وتمويل من معهد نيويورك للتكنولوجيا New York Institute of Technology والكلية العالمية للتكنولوجيا في أبوظبي وناقش المؤتمر التهديدات الاقتصادية والامنية والاجتماعية للجريمة الإلكترونية ووسائل الحماية والتدريب واستعراض التجارب والخبرات المكتسبة في مجال مكافحة الجريمة الإلكترونية.

وتجدر الاشارة إلى أنه في إطار الاعداد لهذا المؤتمر ,عقدة ورشة عمل في ذات الموضوع بتاريخ ١٥ يناير ٢٠١٤ وسمنار في نفس التاريخ وكلاهما في أبوظبي .

مؤتمر الأمن السيبراني: مسقط ٢٣-٢٤مـارس٢٠١٤:Cyber Defence Summit- Mascat ٢٠١٤

عقد هذا المؤتمر في مسقط لمناقشة أهمية الأمن السيبراني بالنظر إلى الاستخدام المتزايد لتكنولوجيا المعلومات والاتصال, حيث صارت الحاجة ملحة لمواجهة الجريمة الإلكترونية في المنطقة وكيفية الوقاية منها, وقد انبثقت من هذا المؤتمر لجان على مستوى خبراء الأمن الإلكتروني من الجهات الحكومية كوزارة الدفاع وغيرها إضافة إلى المصارف وشركات صناعة النفط والغاز لتحديد التحديات الأمنية على الانترنت وكيفية مواجهتها, وإيجاد الحلول لهذه التحديات والتهديدات لصناعة النفط والغاز[١٢٨].

---

١٢٧ Global Cyber Security Conference in Abu Dhabi: National and Corporate Threats, Protection, And Education, March 25,2014.

١٢٨ الجهة التي نظمت المؤتمر هي:

Naseba , Saver Complex , 3rd Floor , 89 Amidala –Horus – Main Road , India .

المؤتمر الاقليمي الثالث للأمن السيبراني Regional Cyber security Summit مسقط ٢٠-٢١أبريل ٢٠١٤:

استضافت سلطنة عمان ممثلة في هيئة تقنية المعلومات العمانية (OCERT) المؤتمر الاقليمي الثالث للأمن السيبراني بالتعاون مع الاتحاد الدولي للاتصالات (ITU) في الفترة من ٢٠-٢١ أبريل ٢٠١٤ في فندق البستان – مسقط , وتولى إدارة المؤتمر المركز العماني الوطني للسلامة المعلوماتية. وناقشت المؤتمر حماية البنيات التحتية الحساسة للمعلومات الوطنية واستهدفت المؤتمر ربط القطاعات العامة والخاصة والأكاديمية بأجندته بمشاركة ٢٥٠متخصصاً و٢٨ متحدثاً في مجالات تكنولوجيا المعلومات والاتصالات والأمن السيبراني من منطقة الشرق الأوسط وقد تمت مناقشة وصياغة توجهات استراتيجية وخطط لمواجهة التهديدات الناشئة للقطاع العالمي والاقليمي. [١٢٩]

المركز الوطني للسلامة المعلوماتية بسلطنة عمان يترأس الاجتماع السنوي السادس للمراكز الوطنية للأمن السيبراني بدول منطقة التعاون الاسلامي في بروناي دار السلام ٢٠- ٢٢أكتوبر ٢٠١٤:

حضر المؤتمر ممثلو دول منظمة التعاون الاسلامي ورؤساء المراكز الوطنية للأمن السيبراني والسلامة المعلوماتية بالدول الأعضاء, الجدير بالذكر أن منظمة التعاون الاسلامي تعد ثاني أكبر تجمع عالمي بعد الأمم المتحدة حيث تضم في عضويتها ٥٧ دولة.

عقد المؤتمر السنوي العام تحت شعار المخاطر الأمنية السيبراني المتجددة والفرص المتاحة, وشارك في المؤتمر عدد من الخبراء والمختصين في مجال الأمن السيبراني من مختلف دول العالم.

ناقش الاجتماع خطة العمل والمبادرات التي تبنتها الدول الأعضاء في مجال الأمن السيبراني وتم اتخاذ القرارات المناسبة لتعزيز الأمن السيبراني بدول منظمة التعاون الاسلامي ,كما تم إقرار عقد الاجتماع السنوي القادم بالتعاون مع منظمة المراكز الوطنية للأمن السيبراني بدول شرق آسيا والتي تضم في عضويتها أكثر من عشرين دولة وسيتم عقد مؤتمر مشترك خلال العام القادم يضم أعضاء كلا المنظمتين في العاصمة الماليزية كوالمبور وذلك لتعزيز التعاون والتنسيق الدولي في مجال الأمن السيبراني[١٣٠].

---

١٢٩ لمزيد من التفاصيل أنظر أوراق عمل ووثائق المؤتمر الإقليمي للأمن السيبراني مسقط ٢٠-٢١ أبريل ٢٠١٤ http://www.reqional cybersecuritysummit.com

١٣٠ المصدر: الموقع الإلكتروني للمركز الوطني للسلامة المعلوماتية cyberdetencesummit-com

مؤتمر الأمن السيبراني- الدوحة ١- ٣ ديسمبر٢٠١٤:

نظمت المؤتمر شركة «تانجينت لينك» البريطانية (Tangent Link UK) تحت رعاية شركة ''معلوماتية'' القطرية أحد المزودين الرائدين لخدمات وحلول تكنولوجيا المعلومات في دولة قطر, وسوف ''معلوماتية '' أهمية مراقبة التهديدات وضرورة تبني نهج استباقي لإدارة أهداف الأمن السيبراني لمؤسسات القطاعين العام والخاص, وحماية مصالح حاملين الأسهم في بيئة رقمية عالمية.

بعض مؤتمرات الجريمة الإلكترونية التي ستعقد خلال عام ٢٠١٥ (للمتابعة):

مؤتمر الأمن السيبراني الدولي الخامس لإنفاذ القانون والصناعة والخبراء الأكاديميين – نيويورك ٥–٨ يناير ٢٠١٥: تستضيف هذا المؤتمر وكالة التحقيقات الفيدرالية الامريكية The Federal Bureau of Investigation (FBI) بمشاركة جامعة فورد هام الأمريكية Fordham University, ويعد المؤتمر فرصة ممتازة لأصحاب المناصب القيادية على المستوى العالمي في مجال تحليل مهددات الجريمة الإلكترونية cyber threats analysis والعمليات operations والبحوث research وانفاذ القانون Enforcement law, وذلك لتوحيد الجهود من أجل عالم أكثر أمناً Create a more secure world[١٣١]

المؤتمر الدولي الأول حول مكافحة جرائم الإنترنت: ٩- ١٥-٢ الرياض - المملكة العربية السعودية:

First International Conference Anti- Cybercrime (ICA2015)

يعقد هذا المؤتمر تحت رعاية خادم الحرمين الشريفين الملك عبدالله بن عبدالعزيز, ويهدف المؤتمر إلى رفع مستوى مكافحة جرائم الإنترنت عن طريق استخدام التقنيات الحديثة والاستفادة من التجارب المحلية والدولية في مجال الإنترنت والأمن السيبراني.

وتشمل أجندة المؤتمر الموضوعات التالية:

- الخصائص والآثار والاتجاهات الحديثة للجريمة الإلكترونية.
- الوعى العام بجرائم الانترنت–الجرائم الإلكترونية والارهاب, ملامح مجرمي جرائم الإنترنت – مفاهيم وتحديات مكافحة الجريمة الإلكترونية – قوانين مكافحة جرائم الإنترنت –

١٣١ لمزيد من المعلومات حول المؤتمر أنظر الموقع الإلكتروني التالي: www. fbi.gov./news/stories/20

تقنيات ووسائل الكشف عن جرائم الإنترنت – دور أمن المعلومات في جرائم الانترنت– حماية البنية التحتية للمعلومات الإلكترونية – تأمين المعاملات الإلكترونية – جمع الأدلة الجنائية الرقمية والتعامل معها – تجارب الدول الأخرى في جرائم الإنترنت. [١٣٢]

مؤتمر الفضاء السيبراني العالمي لاهاي- هولندا - 2015Global Cyberspace Conference 16-17April 2015

أعلن وزير خارجية هولندا أن أكثر من ١٠٠ دولة مدعوة لمؤتمر الفضاء الافتراضي الدولي بالإضافة إلى ممثلي الشركات ومنظمات المجتمع المدني ومن المتوقع أن يحضر المؤتمر ١٣٠٠مشارك.

المؤتمر الدولي السابع للطب الشرعي الرقمي والجرائم الإلكترونية سيول- كوريا الجنوبية / 2015The International Conference on Digital Forensics Cybercrime -October 6-8 -2015 Seoul ,South Korea

سهلت شبكة الإنترنت ارتكاب الجرائم الإلكترونية بتوفيرها طرق الهجمات على أجهزة الحاسوب مع إمكانية عدم التعرف على هوية الجاني, وقد أدت التعقيدات المتزايدة في تقنيات الاتصالات والبنيات التحتية للشبكات إلى صعوبة التحقيق في الجرائم الاليكترونية, نظراً لأن الأدلة على هذه النشاطات غير المشروعة يتم دفنها واخفائها داخل كميات ضخمة من مجلدات البيانات والتي يجب فحصها جميعاً للحصول على الأدلة وكشف الجريمة.

ويعد الطب الشرعي الرقمي والتحقيق في الجرائم الإلكترونية Cybercrime Investigation من المجالات ذات الاهمية البالغة لإنفاذ القانون والأمن القومي وتأكيد المعلومات Information Assurance وهذا المجال متعدد التخصصات, يشمل القانون – علوم الكمبيوتر– التمويل– تحليل البيانات – الشرطة.

ما تقدم ذكره يشكل محاور أجندة المؤتمر الذي يجمع بين الممارسين والباحثين من مختلف المجالات ويوفر فرص العمل والمشاركة الفكرية بين الحضور.

١٣٢ أنظر موقع موسوعة ويكيبيديا الإلكتروني: http://wikcfp.com/cfp/servlet/even

المبحث الخامس
المراكز التقنية والآليات الأخرى الوطنية والإقليمية والدولية ودورها في إعداد البرامج التنفيذية وحماية الأمن السيبراني

إن الحماية الحقيقية الفاعلة للأمن السيبراني تتم من خلال الاستراتيجيات والسياسات والخطط التي تندرج منها البرامج التنفيذية الوطنية والإقليمية والدولية بوصفها أحد الوسائل الرئيسية لمواجهة الجريمة الإلكترونية، ويتطلب إعداد هذه البرامج وتنفيذها وتقييمها آليات تتمثل في إنشاء مراكز متخصصة وطنية وإقليمية ودولية، سنتناول موضوعات هذا المبحث في ثلاثة مطالب كما يلي:

المطلب الأول: المراكز الوطنية الخليجية لحماية الأمن السيبراني: فريق الاستجابة لطوارئ الحاسب الآلي (Computer Emergency Response Team (CERT.

المطلب الثاني: المركز الإقليمي للأمن السيبراني للمنطقة العربية.

المطلب الثالث: التحالف الخليجي لحماية الأمن السيبراني (آلية مقترحة).

المطلب الأول
المراكز الوطنية الخليجية لحماية الأمن السيبراني
فرق الاستجابة لطوارئ الحاسب الآلي

Computer Emergency Response Teams (CERTs)

مواكبة للجهود الدولية والإقليمية في حماية الأمن السيبراني الوطني، تم تأسيس مراكز وطنية لهذا الغرض في عدد كبير من دول العالم وفي غالبية دول مجلس التعاون لدول الخليج العربية، ونقدم فيما يلي تعريفاً موجزاً بهذه المراكز وأهدافها ودورها في حماية الأمن السيبراني ومواجهة الجريمة الإلكترونية.[١٣٣]

دولة الإمارات العربية المتحدة:

مركز الاستجابة لطوارئ الحاسب الآليComputer Emergency Response Centre Team (ae CERT)أنشأت هيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة مركز الاستجابة لطوارئ الحاسب الآلي عام ٢٠٠٧م لتحسين معايير وممارسات أمن

١٣٣ يتم عرض المراكز الوطنية لحماية الأمن السيبراني حسب الترتيب الأبجدي للدول.

المعلومات وحماية البنية التحتية لتقنية المعلومات من مخاطر اختراقات الإنترنت(١٣٤).

الرؤية:

أن يكون هذا المركز في طليعة المراكز الموثوقة التي تنسق العمل من أجل مكافحة جرائم الإنترنت في المنطقة.

المهمة:

- دعم البنية التحتية للاتصالات ونظم المعلومات والمحافظة عليها من تهديدات الجرائم الأمنية على الإنترنت.
- بناء ثقافة آمنة ومحمية في مجال جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة.

الأهداف:

يهدف فريق الاستجابة لطوارئ الحاسبات في الدولة إلى:

- تعزيز قانون مكافحة جرائم تقنية المعلومات والمساعدة في استحداث قوانين جديدة.
- تعزيز الوعى حول أمن المعلومات على مستوى الدولة.
- بناء خبرات وطنية في مجال أمن المعلومات وإدارة الطوارئ وتحرى الأدلة في الحسابات.
- إنشاء مركز اتصال موثوق للإبلا غ عن جرائم تقنية المعلومات في الدولة.
- إنشاء مركز وطني لجمع المعلومات عن التهديدات والمخاطر وجرائم تقنية المعلومات.
- تشجيع إنشاء ومساعدة فرق الاستجابة لحوادث أمن الحاسبات(CERTs) في القطاعات المختلفة.
- التنسيق مع الفرق المحلية والدولية للاستجابة لحوادث أمن الحاسبات ومع المؤسسات ذات الصلة.
- أن يصبح المركز عضواً فعالاً في المؤسسات والمنتديات الأمنية المعروفة.(١٣٥)

ترتيب الدول العالمي للأمن السيبراني: Global Cyber Security Index(GCI) 2014

تم هذا الترتيب العالمي نتيجة لدراسة مشتركة بين الاتحاد الدولي للاتصالات (ITU) ومؤسسة الأبحاث «ABIresearch" للتعرف على مدى مقدرات دول العا لم في مجال الأمن

١٣٤ المصدر: الموقع الإلكتروني لمركز الاستجابة لطوارئ الحاسب الآلي بدولة الإمارات العربية المتحدة (CERT ae). www. aeccert.ae/about-us-ar.p

١٣٥ أنظر الموقع الاليكتروني السابق.

السيبراني«Cyber Security Capabilities» ، وبما أن للأمن السيبراني مجالات تطبيق واسعة تتقاطع في كثير من الصناعات والقطاعات، لذلك يعتمد ترتيب الدول على تحليل مدى تطورها في خمسة محاور وهي:

١- المعايير التشريعية ”Legal Measures“

٢- المعايير التقنية (Technical Measures“

٣- المعاير التنظيمية«Organizational Measures“

٤- بناء القدرات ”Capacity Building“

٥- التعاون الدولي[١٣٦] «International Cooperation ”

وفقاً لمدى مقدرات دول العالم اعتباراً للمعايير أعلاه، جاء ترتيب الولايات المتحدة الأمريكية في المركز الأول وكندا في المركز الثاني واشتركت بقية دول العالم - ١٩٠ دولة - في الترتيب من ٣ إلى ٢٩.

الترتيب العالمي لدولة الإمارات العربية المتحدة في مجال الأمن السيبراني لعام ٢٠١٤:

تم تقييم أداء دولة الإمارات العربية المتحدة في مجال الأمن السيبراني بواسطة الاتحاد الدولي للاتصالات (ITU) بالشراكة مع مؤسسة الابحاث «ABIresearch « وجاء ترتيبها العالمي رقم (١٧) مشترك قبلها ستون دولة من بينهم سلطنة عُمان رقم (٣) مشترك وقطر رقم (٨) مشترك وبعدها ١٣٢ دولة من أصل ١٩٣ دولة من بينها البحرين رقم (١٩) مشترك والمملكة العربية السعودية رقم (١٩) مشترك والكويت رقم (٢٧) مشترك.[١٣٧]

مملكة البحرين:

بالبحث في شبكة الإنترنت لم نجد موقعاً إلكترونياً لمركز وطني بحريني حكومي لفريق الاستجابة لطوارئ أمن الحاسب الآلي، وبالرجوع لقائمة المراكز الوطنية العالمية للاستجابة لطوارئ الحاسب الآلي«List of National CERTs» التي أصدرها معهد هندسة البرمجيات «Software Engineering» «Institute التابع لجامعة كارنيجي ميلون الأمريكية ”Carnegie Mellon University “ لم تتضمن قائمة مراكز CERT

١٣٦ المصدر: الموقع الإلكتروني للاتحاد الدولي للاتصالات (ITU): www.itu.int/en/ITU-D/cybersecrity/pages/GCI-aspx

١٣٧ أنظر المرجع السابق ملحق رقم (٨) .

حول العالم لعام ٢٠١٤ دولة البحرين، ونستنتج من ذلك عدم تأسيس مركز CERT البحرين الحكومي حتى لحظة دخول الموقع الإلكتروني والاطلاع على القائمة.(١٣٨)

القطاع الخاص يؤسس فريق الاستجابة لطوارئ الحاسب الآلي بالبحرين:

بالبحث في شبكة الإنترنت، وبالاطلاع على موقع إدارة مركز البيانات ORG وجدنا أن شركة " تحديث للاستشارات" Reload Consulting Services وهي شركة خاصة مقرها البحرين، قامت بتأسيس مركز الاستجابة لطوارئ الحاسب الآليCERT في ٤ نوفمبر ٢٠١٢ لأول مرة في مملكة البحرين، وتم ذلك بالشراكة مع مجموعة من الشركات البريطانية والأمريكية والهندية، ونظرا لأن هذا المركز يتبع القطاع الخاص بالكامل، وأن الحكومة البحرينية ليست شريكا من خلال مؤسساتها الرسمية ذات الصلة، بالتالي الاتحاد الدولي للاتصالات هو الآخر ليس طرفا في هذه الشراكة الخاصة، وكذلك "معهد هندسة البرمجيات « بجامعة كارنيجي ميلون الأمريكية صاحبة الامتياز في تأسيس مراكز الاستجابة لطوارئ الحاسب الآلي حول العالم (CERTs) (١٣٩) ليس شريكا في تأسيس مركز البحرين خلافا لما جرى عليه الحال في أربعة من دول الخليج ودول أخرى عديدة في العالم، وهذه الأسباب تفسر عدم تضمين مركز البحريني الخاص في قائمة المراكز الوطنية حول العالم التي أعدها معهد هندسة البرمجيات الأمريكي المشار إليه.

أهداف المركز:

- تقديم خدمة كشف البرمجيات الضارة وتحديد مواقعها.
- توفير تنبيهات مبرمجة ومتعمقة تفيد توفير القدرة وسرعة القرار.
- تمكين المنظمات من تعزيز أعمالها ضد العدوى الخبيثة وضمان سمعة مدوناتها.
- يقدم الفريق خدماته التجارية في مملكة البحرين ودول مجلس التعاون الخليجي.(١٤٠)

الترتيب العالمي لمملكة البحرين في مجال الأمن السيبراني لعام ٢٠١٤:

تم تقييم أداء مملكة البحرين في مجال الأمن السيبراني لعام ٢٠١٤ بواسطة الاتحاد الدولي

---

١٣٨ المصدر: قائمة المراكز الوطنية للاستجابة لطوارئ الحاسب الآلي حول العالم، ملحق رقم (٩) .

١٣٩ مجموعة الشركات متعددة الجنسيات التي ساهمت مع الشركة البحرينية « تحديث للاستشارات» في تأسيس « فريق الاستجابة لطوارئ الحاسب الآلي الخاص هي: 1- Varese Secure (UK) 2 - Secure Marx (India) 3- Quays (USA)

١٤٠ أنظر الموقع الإلكتروني السابق، www.cert.org/incident

للاتصالات (ITU) بالشراكة مع مؤسسة الأبحاث (ABIresearch) وجاء ترتيبها العالمي رقم (١٩) مشترك قبلها (٧٥) دولة من بينها حسب الترتيب، سلطنة عُمان رقم (٣) مشترك وقطر رقم (٨) مشترك، وبعدها (١١٧) دولة، من بينها الكويت رقم (٢٧) مشترك.

المملكة العربية السعودية:

المركز الوطني الارشادي لأمن المعلومات: فريق الاستجابة لطوارئ الحاسب الآلي

Saudi Arabia Computer Emergency Response Team (CERT-SA)

تم إنشاء هذا المركز بواسطة هيئة الاتصالات وتقنية المعلومات السعودية Communication and Information Technology Commission ويهدف للكشف عن التهديدات والمخاطر، منع الاختراقات والانتهاك للأمن السيبراني والتنسيق والاستجابة للمعلومات عن حوادث الأمن السيبراني على مستوى المملكة.[١٤١]

الرؤية:vision

أن يكون المركز مرجعية موثوقة ومفوضة بشأن أمن المعلومات في المملكة العربية السعودية.

الرسالة: Mission

- زيادة مستوى الوعى بأمن المعلومات في المملكة العربية السعودية.
- تنسيق الجهود الوطنية نحو ترقية أفضل ممارسات الأمن السيبراني وخلق الثقة بين مجتمع المعلومات «Cyber community".
- المساعدة على التصدي لهجمات وحوادث أمن المعلومات في المملكة.
- أن يكون المركز المرجعية الأساسية referencepoint في مجال أمن المعلومات بالنسبة لمجتمع المعلومات في المملكة العربية السعودية.
- بناء القدرات والمواهب البشرية في مجال أمن المعلومات في المملكة العربية السعودية.
- توفير بيئة موثوقة للتعاملات لبناء الثقة والتعاون مع الجمهور ومع مجتمع المعلومات «Cyber community" في المملكة.[١٤٢]

الترتيب العالمي للمملكة العربية السعودية في مجال الأمن السيبراني لعام ٢٠١٤:

تم تقييم أداء المملكة في مجال الأمن السيبراني لعام ٢٠١٤دلبواسطة الاتحاد الدولي

١٤١ المصدر: الموقع الإلكتروني للمركز الوطني الارشادي لأمن المعلومات بالمملكة العربية السعودية (CERT-SA)– http:cert-gov-sa

١٤٢ أنظر الموقع الاليكتروني السابق.

الاتصالات (ITU) بالشراكة مع مؤسسة اللأبحاث (ABIresearch) وجاء ترتيبها العالمي رقم (١٩) مشترك قبلها (٧٥) دولة من بينها حسب الترتيب سلطنة عُمان رقم (٣) مشترك، قطر رقم (٨) مشترك، دولة الإمارات العربية المتحدة رقم (١٧) مشترك، وبعدها (١١٧) دولة من بينها الكويت رقم (٢٧) مشترك.[١٤٣]

دولة الكويت:

في ١٩ مايو ٢٠١٢ تم افتتاح النسخة الرابعة من مؤتمر ومعرض الكويت لأمن المعلومات» Kuwait Info Security Conference Exhibition« ، وفي كلمة الافتتاح أعلن وزير المواصلات الكويتي عن إنشاء المركز الوطني للاستجابة لطوارئ الحاسب في دولة الكويت (KW-CERT) والذي سيرتبط بالمراكز المماثلة المنتشرة حول العالم.[١٤٤]

وبالبحث في شبكة الإنترنت لم نعثر على موقع إلكتروني باسم مركز (CERT) الكويتي الذي تم إعلان إنشائه في ٢٠١٢/٥/١٩، كما لم نجد أي أخبار أخرى لاحقة عن افتتاح المركز أو ممارسة نشاطاته، وبالرجوع إلى قائمة المراكز الوطنية للاستجابة لطوارئ الحاسب الآليList» of National CERTS« التي أصدرها عام ٢٠١٤ معهد هندسة البرمجياتSoftware« » Engineering Institute التابع لجامعة كارنجي ميلون الأمريكية،[١٤٥] «Carnegie» Mellon University م تتضمن قائمة مراكز CERT حول العالم لعام ٢٠١٤ دولة الكويت، وبذلك يستنتج أن مركز CERT بالكويت الذي تم الإعلان عن إنشائه في ١٩ مايو ٢٠١٢ ربما يكون تحت التأسيس ولم يباشر نشاطه بعد.[١٤٦]

الترتيب العالمي لدولة الكويت في مجال الأمن السيبراني لعام ٢٠١٤:

تم تقييم أداء دولة الكويت في مجال الأمن السيبراني لعام ٢٠١٤بواسطة الاتحاد الدولي للاتصالات (ITU) بمشاركة مؤسسة الابحاث " ABIresearch " وجاء ترتيبها في المركز

١٤٣ أنظر المرجع السابق، قائمة الترتيب الدولي العالمي للأمن السيبراني لعام ٢٠١٤ ، ملحق رقم (٨)

١٤٤ المصدر: الموقع الإلكتروني: Kuwait 10.net/tag/kw-cert

١٤٥ جامعة كارنيجي ميلون الأمريكية صاحبة حق الامتياز في ابتكار وإنشاء مراكز CERT حيث تم إنشاء أول مركز في هذه الجامعة عام ١٩٨٨ في " معهد هندسة البرمجيات " بالجامعة وانتشرت هذه المراكز بعد ذلك حول العالم تحت استشارة وإشراف الجامعة المعنية.

١٤٦ المصدر: قائمة المراكز الوطنية للاستجابة لطوارئ الحاسب الآلي حول العالم، ملحق رقم (٩) وقد تم الاطلاع على هذه القائمة في الموقع الاليكتروني لمعهد هندسة البرمجيات المشار اليه في الهامش (١) أعلاه يوم ٢١ ديسمبر ٢٠١٤ الساعة التاسعة مساءا : www.cert.org/incident

(٢٧) مشترك، وهو المركز الثالث قبل الأخير الذي تشترك فيه (١٣) دولة، ويأتي قبلها (١٦١) دولة من أصل ١٩٣من بينها جميع دول مجلس التعاون لدول الخليج العربية، ومن الواضح أن هذا المركز المتأخر للكويت نتيجة لعدم وجود أو عدم فعالية الآليات والمراكز المتخصصة في سلامة المعلومات والأمن السيبراني ومواجهة الجريمة الإلكترونية.

سلطنة عُمان:

المركز الوطني للسلامة المعلوماتية (Oman) National Information Safety Center

تم في هذا المركز إنشاء **فريق الاستجابة لطوارئ الحاسب الآلي**

(CERT) Computer Emergency Response Team ويتبع لهيئة تقنية المعلومات بسلطنة عُمان وافتتح في إبريل ٢٠١٠.

الرؤية:

أن تكون لسلطنة عُمان قدرات أمن معلومات بمقاييس عالمية تجعل كل مستخدم للحاسب الآلي في السلطنة يشعر بالأمن والسلامة.

مهمة المركز:

- تأهيل كوادر وطنية في مجال الحاسب الآلي والإنترنت من أجل زيادة القدرة على كشف الحوادث الأمنية والاستجابة الطارئة لها.
- تحليل المخاطر والتهديدات الأمنية في فضاء الإنترنت العماني.
- بناء وتعزيز الوعى الأمني في مجال الحاسب الآلي والإنترنت في مؤسسات القطاع العام والخاص وبين المواطنين والمقيمين في السلطنة.

أهداف المركز:

تصبو الأهداف إلى تحقيق الرؤية المتمثلة في توفير بيئة معلوماتية آمنة وفقاً لما يلي:

- العمل كمركز اتصال موثوق للإبلاغ عن أي حوادث أمنية تتعلق بتقنية المعلومات والاتصالات.
- بناء الثقة في استخدام الخدمات الإلكترونية الحكومية.
- بناء الوعى الأمني في فضاء الإنترنت العماني.

- بناء القدرات الأمنية للتعامل مع الحوادث الأمنية المتعلقة بالحاسوب والإنترنت.
- تقديم معلومات دقيقة وآمنة عن التهديدات الأمنية ونقاط الضعف الحالية أو الناشئة.
- تحليل التهديدات الأمنية المحتملة وآثارها.
- توفير تدابير استباقية لتقليل الحوادث الأمنية.
- الاستجابة للحوادث الأمنية والحد من آثارها.
- تشجيع البحث والتطوير في مجال أمن المعلومات.
- التنسيق مع مراكز الاستجابة لطوارئ الحاسوب على الصعيدين الإقليمي والدولي.[١٤٧]

الترتيب العالمي لسلطنة عُمان في مجال الأمن السيبراني لعام ٢٠١٤:

تم تقييم أداء سلطنة عُمان في مجال الأمن السيبراني لعام ٢٠١٤ بواسطة الاتحاد الدولي للاتصالات (ITU) بمشاركة مؤسسة الأبحاث "ABIresearch"، وجاء ترتيبها العالمي رقم (٣) مشترك، وأحرزت الولايات المتحدة الأمريكية المركز الأول، وكندا في المركز الثاني واشتركت ثلاثة دول في المركز الثالث هي استراليا وماليزيا وسلطنة عُمان من أصل (١٩٣) دولة، وبذلك حققت سلطنة عُمان من خلال أجهزتها المختصة بالأمن السيبراني نجاحاً وتفوقا على المستوى العالمي يستحق الثناء والتقدير والمحافظة عليه بالجهود الحثيثة لترقية وتطوير الأداء.[١٤٨]

دولة قطر:

فريق الاستجابة لطوارئ الحاسب الآلي القطري:

" Qatar Cybercrime Emergency Response Team « (Q-CERT)

تم إنشاء "المركز الوطني لأمن المعلومات «National Information Security Center

بواسطة المجلس الأعلى لهيئة تقنية المعلومات والاتصالات القطرية (ict QATAR)[١٤٩] في ديسمبر ٢٠٠٥ بالتعاون مع معهد هندسة البرمجيات في جامعة كارنيجي ميلون الأمريكية (CERT/CC) «The CERT Coordination Center لمواجهة تهديدات الجريمة الإلكترونية وتحديات الأمن السيبراني، وكوسيلة لبناء مقدرات التعامل مع معلومات البنيات التحتية الحرجة في دولة قطر، وقد أصبح المركز(Q-CERT) مسؤولاً عن أمن واحتياجات

---

١٤٧ المصدر: الموقع الإلكتروني للمركز الوطني للسلامة المعلوماتية بسلطنة عمان: www.cert.gov.om/about وأنظر كذلك قائمة مراكز CERT حول العالم، ملحق رقم (٩)

١٤٨ المصدر: المرجع السابق، قائمة الترتيب الدولي العالمي للأمن السيبراني لعام ٢٠١٤، ملحق رقم (٨)

١٤٩ Supreme Council of Information and Communication Technology (ict QATR)

حماية معلومات الأمة القطرية وتأمين المجتمع المحلي وتوجيهه نحو إيجابيات التقنية.

ويعمل المركز لتنسيق استخدام التقنية من خلال الممارسات الجيدة والسياسات المعيارية «Standard Policies» وتقليل المخاطر وتقديم المعلومات القيمة بشأن حماية الأمن السيبراني.[١٥٠]

الرؤية: Vision

- أن يعُرف مركز (Q-CERT) رائداً في قطر والمنطقة في ترقية معايير تقنية المعلومات «IT Security Standard›s" والممارسات «Practices» والمنتجات«Products " والخدمات Services لتحقيق أمن البنيات التحتية الحرجة لتقنية المعلومات.
- مصدر موثوق لأمن المعلومات.
- شريك موثوق به وواثق من مقدراته على الاستجابة في حوادث الأمن السيبراني«Cyber security incidents»
- رائد في بناء وتأهيل القدرات البشرية في مجال الأمن السيبراني.

الرسالة: Mission

- تقديم معلومات دقيقة وبالسرعة المطلوبة عن التهديدات القائمة والمتوقعة لأمن المعلومات ومواطن الضعف في الأنظمة والأجهزة وقابلية الاختراق.
- الاستجابة للتهديدات وقابلية الاختراق أو الهجمات الإلكترونية الموجهة للجمهور.
- ترقية معايير أمن المعلومات «Security Standards» والعمليات «Processes" والطرق «Methods» وأفضل الممارسات والوسائل.[١٥١]

الترتيب العالمي لدولة قطر في مجال الأمن السيبراني لعام ٢٠١٤:

تم تقييم أداء دولة قطر في مجال الأمن السيبراني لعام٢٠١٤ بواسطة الاتحاد الدولي للاتصالات (ITU) بمشاركة مؤسسة الأبحاث «ABIresearch"، وجاء ترتيبها العالمي رقم (٨) مشترك، قبلها (٢٣) دولة من بينها سلطنة عُمان رقم (٣) مشترك، وبعدها (١٦٩) دولة من بينها على التوالي دولة الإمارات العربية المتحدة رقم (١٧) مشترك، ومملكة البحرين رقم (١٩) مشترك، والمملكة العربية السعودية رقم (١٩) مشترك، ودولة الكويت رقم (٢٧) مشترك.[١٥٢]

---

١٥٠ المصدر: موقع Q-CERT الإلكتروني: www.qcert.orq/about-q-cert

١٥١ أنظر المرجع السابق، الموقع الإلكتروني لمركز Q-CERT.

١٥٢ أنظر المرجع السابق، قائمة الترتيب الدولي العالمي للأمن السيبراني لعام ٢٠١٤ ، ملحق رقم (٨) .

المطلب الثاني

المركز الإقليمي للأمن الاليكتروني للمنطقة العربية

Arab Area Cyber Security Regional Center

نتناول فيما يلي دور الاتحاد الدولي للاتصالات (ITU) في إنشاء المركز الإقليمي للأمن الإلكتروني للمنطقة العربية ومن ثم التعريف بالمركز وأهدافه واستراتيجيته ودوره في تأهيل الكوادر وتطوير البرامج والحلول التقنية ومدى الجاهزية الأمنية للمركز.

الاتحاد الدولي للاتصالات International Telecommunication Union: (ITU)

هو ثاني أقدم تنظيم عالمي ما زال قائما – التنظيم الاقدم عالمياً فهو اللجنة المركزية للملاحة في نهر الراين – وقد تم تأسيسه عام ١٨٦٥م ، وكانت مهمته الرئيسية تتعلق بالاتصالات السلكية واللاسلكية والآن هو إحدى وكالات الأمم المتحدة المتخصصة في تقنية المعلومات والاتصالات ومقره جنيف، سويسرا، ومهمته الرئيسية هي ما جاء في شعاره «الالتزام بتوصيل العالم» Committed to Connecting The World من خلال شبكات النطاق العريض المتاحة في كل مكان بأسعار ميسورة لتعزيز التنمية الاجتماعية والاقتصادية.[١٥٣]

أنشطة الاتحاد الدولي للاتصالات في مجال الأمن السيبراني: ITU Cyber Security Activities

يضطلع الاتحاد الدولي للاتصالات، منذ القمة العالمية لمجتمع المعلومات ومؤتمر المندوبين المفوضين التي عقدت عام٢٠١٠، بدور أساسي يتمثل في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، ففي القمة العالمية لمجتمع المعلومات[١٥٤]، عهد رؤساء الدول وقادة العالم إلى الاتحاد بأداء دور الميسر (Facilitator) لتنفيذ خطط العمل التي ترمى إلى بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.[١٥٥]

---

١٥٣ أنظر المرجع السابق، قائمة الترتيب الدولي العالمي للأمن السيبراني لعام ٢٠١٤ ، ملحق رقم (٨) .

١٥٤ أنظر الموقع الإلكتروني للاتحاد الدولي للاتصالات: www.itu.int/or/action/pages

١٥٥ world summit Information Society (wises) Geneva, 10- 14 May 2010

المركز الإقليمي للأمن الإلكتروني للمنطقة العربية: Arab Area Cyber Security Regional Center

تم التوقيع على اتفاقية المركز بتاريخ ١٥ ديسمبر ٢٠١٢ بين الاتحاد الدولي للاتصالات (ITU) وهيئة تقنية المعلومات باستضافة سلطنة عُمان '' للمركز الإقليمي للأمن الإلكتروني للمنطقة العربية'' ، وقد تم بموجب مبادرة الاتحاد الدولي للاتصالات ومنظمة امباكت[١٥٦] تفويض المركز الوطني للسلامة المعلوماتية بالسلطنة القيام بإدارة وتشغيل المركز الإقليمي للأمن الإلكتروني للمنطقة العربية، إلى حين إنشائه على غرار مراكز إقليمية مماثلة في دول الاتحاد الأوربي وآسيا وغيرها من الأقاليم الأخرى.

أهداف المركز الإقليمي للأمن الإلكتروني للمنطقة العربية:

١- تقديم الخدمات والمبادرات التي تنفذها منظمة «إمباكت « والاتحاد الدولي للاتصالات للمنطقة العربية ، لتحسين قدرات الأمن الإلكتروني في المنطقة عن طريق التنسيق الإقليمي في هذا المجال.

٢- يقوم المركز بدور المنسق الإقليمي لجميع الفعاليات والأنشطة والمشاريع المتعددة والتي يتبناها وينفذها الاتحاد الدولي للاتصالات ومنظمة ''إمباكت'' في مجال الأمن الإلكتروني في المنطقة العربية.

استراتيجية عمل المركز الإقليمي للأمن الإلكتروني للمنطقة العربية:

يقوم المركز بتبني الأجندة العالمية للأمن الإلكتروني التي اعتمدها الاتحاد الدولي للاتصالات والتي تتناول الأمن الإلكتروني من عدة جوانب:

١. ضرورة إيجاد مركز وطني في كل دولة للتعامل مع تحديات الأمن الإلكتروني ويشرف على مبادرات وبرامج الأمن الإلكتروني على المستوى الوطني.

٢. العمل مع الشركاء بالجهات المختصة على سن القوانين التي تنظم التعاملات الإلكترونية والتي تُجرِّم الاستخدام غير المشروع للتقنية.

٣. تدريب وتأهيل وتنمية القدرات وتطويرها في مجال الأمن الإلكتروني.

٤. توفير أحدث التقنيات للأمن الإلكتروني.

٥. تفعيل التعاون الدولي والإقليمي في هذا المجال.

---

١٥٦ منظمة امباكت Impact هي الذراع التنفيذي لمبادرات الأمن السيبراني للاتحاد الدولي للاتصالات.
International Multilateral Partnership Against Cyber Threats (Impact)

تفعيل الاستراتيجية:

يتم تفعيل الاستراتيجية من خلال القيام بالآتي:

١. أن يعمل المركز باعتباره مركزا رئيسيا للأمن الإلكتروني بالمنطقة العربية.
٢. مساعدة الدول النامية في المنطقة العربية في تنفيذ مبادرات الأمن الإلكتروني بهذه الدول.
٣. تعزيز الوعى بالأمن الإلكتروني لدى مؤسسات البنى الأساسية بالمنطقة العربية.
٤. إشراك صناع القرار في هذه الدول في مساندة مبادرات الأمن الإلكتروني وتوجيه البرامج بما يتناسب مع طبيعة واحتياجات المنطقة العربية.
٥. تفعيل وتعزيز التعاون الإقليمي في هذا المجال وتشجيع تبادل التحذيرات والإنذارات حول المخاطر والتهديدات الأمنية الإلكترونية ووسائل الحماية منها.
٦. تشجيع برامج البحث والتطوير في مجال الأمن الإلكتروني بالمنطقة العربية.
٧. إجراء برامج قياس الجاهزية للتعامل مع المخاطر الأمنية الإلكترونية ومدى الكفاءة في الحد من نطاق تأثيرها.

تأهيل كوادر المركز الإقليمي للأمن الإلكتروني:

تضمنت اتفاقية إنشاء المركز التأكيد على تأهيل الكوادر العاملة كما يلي:

١- تخصيص عدد من المنح التدريبية التخصصية التي يوفرها شركاء المنطقة العالميين والمتخصصين في مجال الأمن الإلكتروني.
٢- عقد ورش عمل ودورات تدريبية تخصصية لتأهيل الكوادر المهنية في السلطنة.
٣- استضافة كوادر المراكز الوطنية للسلامة المعلوماتية بالمنطقة العربية ضمن برامج التدريب في مقر منظمة (إمباكت) لاكتساب المهارات والخبرات العملية.

تطوير البرامج والحلول التقنية:

يساهم المركز في تطوير مجموعة من البرامج والحلول التقنية في مجال الأمن الإلكتروني، وتأهيل مجموعة من موظفي المركز الوطني للسلامة المعلوماتية بالسلطنة وتزويدهم بالكفاءات والمهارات اللازمة للتعامل مع مخاطر الأمن الإلكتروني لتعزيز عمل المركز الإقليمي، إضافة إلى الحصول على آخر التحديثات والتقارير والحلول التقنية في مجال الأمن الإلكتروني.

الخدمات التي سيقدمها المركز للمنطقة العربية:

١- المساعدة في تأسيس وإنشاء المراكز الوطنية للسلامة المعلوماتية (CERT).

٢- الاستجابة للطوارئ المعلوماتية بالدول العربية التي لم تستكمل إنشاء مركز السلامة المعلوماتية.
٣- تقديم الاستشارات في مجال الأمن الإلكتروني لدول المنطقة.
٤- التدريب التخصصي والاحترافي في مجال الأمن السيبراني.
٥- عقد الندوات والمؤتمرات وورش العمل.
٦- التقييم الأمني لمستوى الأمن الإلكتروني بالمنطقة ومساعدة الدول في سد الفجوة في هذا المجال.
٧- توفير الوسائل والبرامج التقنية في مجال الأمن الإلكتروني لدول المنطقة.
٨- المشاركة في التحذيرات والتنبيهات الأمنية حول المخاطر والتهديدات التي تواجهها المنطقة.
٩- الاستجابة للحوادث الأمنية المعلوماتية التي تتعرض لها دول المنطقة.[١٥٧]

وتجدر الإشارة إلى أن المركز الإقليمي للأمن الإلكتروني للمنطقة العربية يتيح الفرصة للسلطنة لتكون جزءاً من المبادرات العالمية للاتحاد الدولي للاتصالات وشركائه العالميين في مجال الأمن الإلكتروني.

الجاهزية الأمنية للمركز الإقليمي للأمن الإلكتروني:

أبرز البرامج والخطط التي يعمل المركز على تنفيذها كما يلي:

١- تعزيز جاهزية التأهب والقدرة على الاستجابة للتهديدات الإلكترونية وجرائم الإنترنت في دول المنطقة من خلال تعزيز قدرات التعرف على المخاطر الأمنية والمعلوماتية والتصدي لها.
٢- إعداد مجموعة من الإجراءات والسياسات الخاصة بحماية المؤسسات الحكومية ومؤسسات البنى التحتية.

خطط المركز:

يخطط المركز للقيام بالآتي:

١- إنشاء خارطة طريق للمنطقة العربية في مجال الأمن الإلكتروني.
٢- بناء القدرات وتعزيز الوعى والثقافة الأمنية والمعلوماتية.
٣- إعداد برامج تقييم الجاهزية للتعامل مع المخاطر والحوادث الأمنية المعلوماتية للمراكز الوطنية بدول المنطقة.

---

١٥٧ المصدر: الموقع الإلكتروني لهيئة تقنية المعلومات بسلطنة عُمان، عمان الرقمية: /http//ita.gov.om/it portal- ar

المطلب الثالث
الآليات الأخرى لحماية الأمن السيبراني:
التحالف الخليجي لحماية الأمن السيبراني
(آلية مقترحة)

مبررات التحالف الإقليمي الخليجي لحماية الأمن السيبراني:

تكمن المبررات في الاستفادة من تجارب التعاون الدولي والإقليمي في إعداد وتنفيذ الاستراتيجيات والسياسات والخطط والبرامج التنفيذية لمواجهة الجريمة الإلكترونية، وذلك نظراً لأن الجريمة الإلكترونية مشكلة عالمية تتطلب استنفاراً مدروساً واستجابة منسقة لتحقيق متطلبات التعاون الدولي والإقليمي الفعال لمواجهة هذه الظاهرة، عرضنا في المطلب الثاني من المبحث الرابع كيفية تضافرت جهود مجموعة الدول الثمانية (G-8) – منذ تأسيسها عام ١٩٩٧– لمواجهة الجريمة الإلكترونية وأسفرت جهودها المكثفة عن إصدار اتفاقية مجلس أوربا للجريمة الإلكترونية. ونشأت بموجب هذه الاتفاقية آليات ومنظمات عديدة من أجل التعاون الدولي لوضع الاستراتيجيات والسياسات والخطط والبرامج التنفيذية لمواجهة الجريمة الإلكترونية سبق الإشارة إليها، ونتناول أهمها فيما يلي:

أولاً: التحالف الدولي لحماية الأمن السيبراني:

نشأت منظمة التحالف الدولي لحماية الأمن السيبراني[١٥٨] من أجل تعزيز التعاون الدولي لمواجهة الجريمة الإلكترونية من خلال إعداد وتقديم وتمويل برامج تنفيذية عملية، ووقعت في نوفمبر ٢٠١١ مذكرة تفاهم للعمل في شراكة مع أمانة الكومنولث لتقنية المعلومات والاتصالات، وكانت رؤية هذه الشراكة أن يعمل التحالف الدولي لحماية الأمن السيبراني (ICSPA) والشركات الأعضاء والسلطات المختصة بإنفاذ القانون لدعم دول رابطة الكومنولث والدول الأخرى التي تطلب المساعدة في أربعة مجالات رئيسية من أجل محاربة الجريمة الإلكترونية وهي:

---

١٥٨ منظمة التحالف الدولى لحماية الأمن السيبراني: The International Cybersecurity Protection Alliance (ICSPA) وهي منظمة عالمية غير ربحية تم تأسيسها في بريطانيا في نوفمبر ٢٠١١ لتوجيه التمويل والخبرات والمساعدة مباشرة لمساعدة وحدات انفاذ قانون، الجرائم الإلكترونية في الجرائم المحلية والدولية، وتضم المنظمة شركات وطنية وأخرى كبيرة متعددة الجنسيات، إضافة شركاء انفاذ القانون مثل اليورو بول) والمنظمات الدولية ذات الصلة، وتشمل عضوية هذا التحالف مجموعة من الشركات العالمية الرائدة في مجالات تقنية وأمن المعلومات وشركات الاتصالات.
اليورو بول هو المنظمة الشرطة الأوربية التي تساعد الاتحاد الأوربي في مكافحة الجريمة المنظمة.

١- الأطر التشريعية والقوانين السيبرانية Cyber Laws والعدالة وخدمات النيابة العامة (الادعاء العام).

٢- تعزيز القدرة على إنفاذ القانون في مجال الوقاية والكشف والتحقيق في الجريمة الإلكترونية.

٣- توفير الحماية للفضاء الإلكتروني للحكومة وللبنيات التحتية الوطنية.

٤- المساعدة بالمعلومات العامة والتوعية والتدريب حول قضايا الأمن السيبراني تستهدف المواطنين والشركات الصغيرة والمتوسطة الحجم.[١٥٩]

ثانياً: برامج مبادرة الكومنولث لمواجهة الجريمة الإلكترونية:

تم تنفيذ المساعدات والبرامج المشار إليها في الفقرة (أولاً) كجزء من تنفيذ مبادرة الكومنولث للجرائم السيبرانية (CC1) Commonwealth Cybercrime Initiative وقد حصل برنامج العمل هذا على موافقة ٥٤ من رؤساء حكومات الكومنولث أثناء اجتماعهم في بيرث استراليا في أكتوبر ٢٠١١.

بدأ العمل في تنفيذ برامج الكومنولث في غرب أفريقيا في عام ٢٠١٢ وأدى نجاح أول عملية إلى أن دولاً أخرى في أفريقيا ومنطقة البحر الكاريبي طلبت المزيد من الجهود في هذا الجانب وبدأ العمل فعلاً في نهاية عام ٢٠١٢ واستمر بعد ذلك.

ثالثاً: الشراكة بين اليورو بول والتحالف الدولي لحماية الأمن السيبراني:

في أوربا بدأ التحالف الدولي لحماية الأمن السيبراني العمل مع اليوروبول كشريك استراتيجي في مجال إنفاذ القانون (Europol) ، وسوف يقوم التحالف بتنفيذ مشاريع في جميع أنحاء أوربا والدول المحيطة والمجاورة لمساعدة الحكومات ووكالات إنفاذ القانون والأعمال التجارية والمواطنين بتقديم برامج الجريمة الإلكترونية Cybercrime والأمن السيبراني Cybersceurity.

ضرورات التحالف الخليجي للحماية من الجريمة الإلكترونية :

بما أن تهديدات الجريمة الإلكترونية المستمرة العابرة للحدود الوطنية تشمل أهدافها اقتصاديات دول مجلس التعاون لدول الخليج العربية وبنياتها التحتية، حيث أصبح الاعتماد على الكمبيوتر وبرامج الكمبيوتر والإنترنت بدرجة عالية في كافة المجالات الحيوية..

---

١٥٩ يورو بول أو Europol هي منظمة الشرطة الأوربية الجنائية.

وإذ تضاعف عدد مستخدمي الإنترنت في دول الخليج الستة بالمقارنة مع عدد السكان بمتوسط ٨٣٪ من إجمالي عدد السكان البالغ ٤٩,٨٣٢,٩٤٢ نسمة..[١٦٠]

وإذ شهد عام ٢٠١٢ هجمات الإلكترونية على مؤسسات إنتاج النفط في المملكة العربية السعودية وقطر ودولة الإمارات العربية المتحدة[١٦١]، وإذ بلغت خسائر المملكة العربية السعودية عام ٢٠١٣ مبلغ ٥٢٧ مليون دولار.

كل ما تقدم من معطيات حول التجارب الدولية في مجال التعاون والتحالف لمواجهة الجريمة الإلكترونية إضافة إلى التهديدات الاقتصادية والاجتماعية المستمرة للأمن السيبراني في منطقة الخليج العربي بسبب غياب استراتيجيات الحماية أو اعتقاد المخترقين بعدم توفر برامج الحماية الكافية للأمن السيبراني، يجعل دول مجلس التعاون لدول الخليج العربية في ظروف مشابهة لدول مجلس أوربا التي تحالفت بإنشاء اتفاقية مجلس اوروبا للجريمة الالكترونية وكذلك تتشابه الظروف التي أدت لقيام» التحالف الدولي لحماية الامن السيبراني» بشراكة دول الكومنولث واليورو بول. إضافة إلى ما تقدم، أن تقييم مستوى حماية الأمن السيبراني الذي قام به الاتحاد الدولي للاتصالات (ITU) وشركة ABlreearch قد كشف مستوى الحماية في دول مجلس التعاون لدول الخليج العربية وقد فصلنا ذلك في المطلب الأول من هذا المبحث الرابع، حيث وضح تفوق سلطنة عمان بإحرازها المركز الثالث عالمياً وأحرزت قطر المركز رقم (٨) مشترك ودولة الإمارات العربية المتحدة رقم (١٧) مشترك ومملكة البحرين والمملكة العربية السعودية رقم (١٩) مشترك والكويت رقم (٢٧) مشترك وهو المركز الثالث قبل الأخير.

وبما أن دول مجلس التعاون لدول الخليج العربية تتمتع بطفرة اقتصادية هائلة وتنتج خمس إنتاج النفط العالمي ما نسبته ٢١,٣٠٪ وتعد قطر ثالث أكبر احتياطي للغاز الطبيعي في العالم بنسبة ١٤,٤٪ من إجمالي الاحتياطي العالمي، فإن البنيات التحتية لصناعة النفط والغاز بصفة خاصة ، وغيرها من مؤسسات القطاع العام والخاص تتطلب تحسين مستوى الأمن السيبراني بكل الوسائل المتاحة في المجال الدولي والإقليمي.

---

١٦٠ أنظر الإحصائية، ملحق رقم (٤)..

١٦١ أنظر تقرير شركة نورتن لعام ٢٠١٢ Norton Cybercrime Report. September 2012

إنشاء آليات تنفيذ برامج الحماية من الجريمة الإلكترونية:

يتطلب ايجاد آليات ضرورة لاستلهام واستصحاب تجرية منظمة» التحالف الدولي لحماية الأمن السيبراني» في وضع السياسات والتخطيط البرامج التنفيذية الدولية والاقليمية والوطنية لمواجهة الجريمة الالكترونية في دول الكومنولث والدول الأخرى، ونقترح استفادة دول مجلس التعاون لدول الخليج العربية من المبادئ الاساسية لهذه البرامج التي تطبق في ٥٤ دولة من دول الكومنولث. ونقترح انشاء منظمة خليجية تقتبس ما تراه مناسبا من المنهج والمعايير التي اتبعتها منظمة التحالف الدولي لحماية الامن السيبراني (ICSPA) ومبادئ وأنشطة اتفاقية مجلس أوربا للجريمة الالكترونية وتقترح أن تحمل المنظمة المقترحة اسم التحالف الخليجي لحماية الأمن السيبراني) Gulf Cooperation Council Cybersecurity Protection Alliance (GCCCPA) ويتم الاتفاق على نظامه الاساسي وإجازته في شكل اتفاقية في مؤتمر رفيع المستوى يعقد لهذا الشأن.

أهداف التحالف الخليجي المقترح لحماية الأمن السيبراني المقترح:

تتمثل أهداف التحالف (المقترح) في الآتي:

- تعزيز السلامة والأمن السيبراني للقطاع العام والخاص، من خلال المساعدة في تقديم الموارد والخبرات من القطاع العام والخاص لدعم سلطات إنفاذ القانون المحلية والدولية ومقوماتها في جهودهم للحد من ضرر الجريمة الإلكترونية، حيث ذكرت دراسة متخصصة[١٦٢] أنه بحلول عام ٢٠١٧ م سوف تصل تكلفة الامن السيبراني العالمي ١٤٥,١ مليار بالمقارنة مع ٦٣,٧ مليار دولار عام ٢٠١١م.
- زيادة تمويل القطاع العام من الحكومات التي ترغب في رفع طاقات وقدرات وحدات الجريمة الالكترونية.
- تنفيذ تدابير لتحسين مرونة الإنترنت عبر البنيات التحتية الوطنية الحيوية في الدول التي تواجه مشكلات وتحديات في هذا الجانب.

البرامج التنفيذية الخليجية الدولية (المقترحة) لمواجهة الجريمة الإلكترونية:

١- تحديد الدول التي يتم استخدامها كقواعد تنطلق منها جرائم الإنترنت وأن تكون هذه الدول على استعداد للتعاون الدولي في هذا المجال وتلقي المساعدات الخارجية الضرورية.

١٦٢ انظر الموقع الالكتروني GO-Gulf : http://www.go-gulf.com/blog/cybe.

٢- تحديد البنيات التحتية والمؤسسات العامة والخاصة والشركات متعددة الجنسيات العاملة في الدول التي تعتبر أهدافا للجريمة السيبرانية وكذلك تحديد الشركات المتعددة الجنسيات في تلك الدول التي تنطلق منها هجمات الجريمة الإلكترونية.

٣- توفير التمويل من الدول أعضاء (التحالف الخليجي لحماية الأمن السيبراني Cyber Security ومن الدول الأخرى التي تستفيد أكثر من مقدرات اكثر نجاحا، وقابلية لإنفاذ قوانين مكافحة الجريمة الإلكترونية.

٤- العمل مع الشركات الأعضاء في التحالف الخليجي والحكومات الأجنبية التي تم تحديدها على أنها على استعداد لقبول المساعدة لتوجيه التمويل والمساعدة لدعم وحدات انفاذ قوانينها المنوط بها مكافحة الجريمة الالكترونية.

٥- تشكيل شبكة دولية تربط بين حكومات التحالف الخليجي لحماية الأمن السيبراني، وأعضاء التحالف من الشركات ووحدات انفاذ القانون وذلك لتعزيز المساعدات المقدمة وابتكار الممارسات الجيدة في جوانب هامة تتعلق بتقنيات عمليات الجريمة الإلكترونية. cybercrime operating techniques

٦- تكوين شراكات مع المنظمات القائمة التي تتفق اختصاصاتها مع مبادرة التحالف الخليجي لحماية الأمن السيبراني مثل: الانتربول- اليورو بول- الرابطة الدولية لرؤساء الشرطة والهيئات المماثلة داخل مجتمع الأعمال الدولي.

الفوائد التي تعود على الشركات متعددة الجنسيات من البرامج التنفيذية الخليجية الدولية (المقدمة) لحماية الأمن السيبراني:

من خلال تقديم هذا النوع من المساعدة بعناية مركزة لوحدات انفاذ القانون في الدول التي تواجه تحديات كبيرة فان الشركات متعددة الجنسيات سوف تحقق الفوائد التالية:

١- تحسين قدرا ت مكافحة الجرائم السيبرانية في الدول التي تعاني من الجريمة السيبرانية والتي تعمل بها تلك الشركات متعددة الجنسيات.

٢- اجراء عمليات تنفيذ للقانون أكثر نجاحا في الدول التي تتلقى المساعدة من التحالف ومن المتوقع انخفاض معدلات الهجمات الالكترونية ضد الشركات العاملة في أسواق تلك الدول.

٣- تقديم المساعدة محليا للدول التي تعمل فيها الشركات متعددة الجنسيات.

٤- العمل مع كبار المسؤولين في الدول الأعضاء في التحالف الخليجي لحماية الامن السيبراني (المقترح) لتمكين التحالف من تطوير مبادرات جديدة في السياسة العامة للتشريعية والمساعدة في تقديم برامج اكثر فاعلية لمكافحة الجريمة الإلكترونية.(١٦٣)

الفوائد التي تجذبها منظمات إنفاذ القانون والحكومات وضباط وموظفي السلطات المختصة بمكافحة الجريمة الإلكترونية من البرامج التنفيذية المقترحة:

١- تحسين قدرات مكافحة جرائم الانترنت.

٢- تحسين فرص التدريب وتبادل المعرفة مع سلطات إنفاذ القانون (الإدعاء العام) مع الدول الأخرى.

٣- تبادل الخبرات الجيدة والمعلومات دوليا بشأن الاساليب الاجرامية السيبرانية الجديدة والمنهجيات.

٤- تحسين سرعة وكفاءة وفاعلية انشطة مساعدات انفاذ القانون الدولية المتبادلة فيما يتعلق بالاستيلاء على الأصول الرقمية التي يجري بشأنها التحقيق بواسطة الادعاء العام.

٥- فهم أفضل لتأثير الجريمة السيبرانية على الشركات الأجنبية المتعددة الجنسيات العاملة في الدول الأعضاء والدول ذات الصلة.

٦- اتخاذ موقف أكثر صرامة في مواجهة مجرمي الإنترنت الذين يستهدفون بلدانهم مما يحقق ردع الجريمة المنظمة الأجنبية التي تنطلق هجماتها السيبرانية ضمن دائرة الاختصاص القضائي. (١٦٤)

الفوائد التي تعود على الدول المشاركة في التحالف والدول الأخرى المتعاونة:

١- تحسين تبادل المعرفة والتعاون في قضايا الجريمة السيبرانية مع الدول الأخرى.

٢- المكافحة الجادة للجريمة الإلكترونية لتشجيع الاستثمار الخارجي الجديد من قبل الشركات متعددة الجنسيات وسوف يساعد ذلك على تعزيز وجود الشركات الأجنبية القائمة بتوفير الثقة لتوسيع نطاق عملياتها.

٣- حملات التوعية الأمنية بمخاطر استخدام الإنترنت تساعد مجتمع دول مجلس التعاون

---

١٦٣ نفس المرجع السابق ، انظر Benefits to multi-national companies

١٦٤ Michael E. Porter, Mark R-Kramer, Creating Shared Value, Harvard Business Review, January-Feb,2011 edition.

لدول الخليج العربية ليصبح الجميع في القطاع العام والخاص أكثر وعياً بالتهديدات التي يواجهونها على الإنترنت.

٤- القدرة على تقديم الخدمات الحكومية لأفراد المجتمع باستخدام شبكة الإنترنت وفقاً لتدابير أمنية تساعد على تحسين بيئة الاستخدام وتحسين القدرة على اكتشاف الجريمة الإلكترونية والتعامل معها.

٥- القدرة المتزايدة للدفاع عن البنى التحتية الوطنية من هجمات الجرائم السيبرانية مما يحقق مزيداً من الفرص لتحقيق الازدهار الوطني من خلال تحسين بيئة الإنترنت.

وتكون مساعدات البرامج التنفيذية الخليجية الدولية، التي يقدمها التحالف الخليجي لحماية أمن الإنترنت Gulf Co-operation Council Cybersecurity Protection Alliance (GCCCPA) (المقترح) في شكل الخبرات التقنية والتدريب على تقنيات جرائم الإنترنت والتسويق الإعلامي وحملات الاتصالات لتعزيز وتحسين الوعي الأمني للإنترنت.[١٦٥]

---

١٦٥ Michael E. Porter, Mark R-Kramer, Creating Shared Value, Harvard Business Review, January-Feb,2011 edition

الخاتمة

النتائـــج:

- تأكد أن الجريمة الإلكترونية ظاهرة إجرامية حديثة وليدة التطورات الهائلة والمتلاحقة في نظم تقنية المعلومات والاتصالات، وهي جريمة عابرة للحدود ويمكن ارتكابها من أي مكان في العالم عبر شبكة الإنترنت، وتتميز بسهولة إخفاء أدلتها، إضافة إلى تعقيدات التحقيق فيها وصعوبة ضبط مرتكبيها، وصارت مشكلة عالمية تهدد أمن المجتمع الدولي.
- ارتفعت معدلات الجريمة الإلكترونية بشكل ملحوظ منذ عقد التسعينات من القرن الماضي، وفي عام ١٩٩٧قامت مجموعة الدول الثمانية G-8 بالتحرك الدولي لمواجهة الأزمة.
- أثمرت جهود مجموعة دول G-٨ بالتوقيع على اتفاقية مجلس أوربا للجريمة الإلكترونية في ٢٣ نوفمبر ٢٠٠١ بوصفها أول مبادرة دولية في هذا الشأن حيث وقعت عليها ٤٥ دولة من الدول الأعضاء في مجلس أوربا البالغ عددها ٤٧ دولة بالإضافة إلى ثلاثة عشرة دولة غير أعضاء في المجلس.
- استجابة للجهود الدولية لمواجهة الجريمة الإلكترونية، أصدرت دول مجلس التعاون لدول الخليجي العربية تشريعات لمواجهة الجريمة الإلكترونية في الفترة من ٢٠٠١ إلى ٢٠١٤ ، وتتفق هذه التشريعات في مفهوم الجريمة الإلكترونية وأنواعها ونصت على الأفعال التي يجرمها التشريع والعقوبات المحددة لها.
- ثبت عدم حماس الدول الأوربية والغربية الكبرى الموقعة على اتفاقية مجلس أوربا للجريمة الإلكترونية للتصديق على الاتفاقية وإدخالها حيز النفاذ في الوقت المحدد، حيث أن ٣٠٪ من الدول الموقعة على الاتفاقية صدقت عليها ونفذتها بعد مرور ٥ إلى ٨ سنوات من فتحها للتوقيع في ٢٠٠١/١١/٢٣، وأن ٣٠٪ أخرى من الدول الأعضاء صدقت عليها وأدخلتها حيز النفاذ بعد مرور ٩ إلى ١٣ سنة من فتحها للتوقيع، أي أن ٦٠٪ من الدول الأعضاء الموقعة على الاتفاقية أدخلتها حيز النفاذ بعد فترة تراوحت بين ٥ إلى ١٣ سنة، مما يؤكد التباطؤ وعدم الحماس الذي كان من نتائجه الارتفاع الكبير في معدلات الجريمة الإلكترونية وفي حجم خسائرها الذي بلغ ٤٥٠ مليار دولار عام ٢٠١٣.

- الهجمات الإلكترونية المدمرة على جمهورية استونيا عام ٢٠٠٧ دقت ناقوس الخطر وتنبه المجتمع الدولي لضرورة تكثيف الجهود لإيجاد الحلول والمعالجات لمواجهة الجريمة الإلكترونية، ومنذ العام ٢٠٠٨ بدأت الدول في إعداد استراتيجيات مكافحة الجريمة الإلكترونية، وحتى عام ٢٠١٤ أعدت ثمانية عشرة دولة أوربية من أصل ٤٧ دولة استراتيجيات للجريمة الإلكترونية و١٨ دولة أخرى من خارج أوربا من بينها الولايات المتحدة الأمريكية وكندا واستراليا واليابان ولا تتضمن القائمة دولة عربية وتجد الإشارة إلى أن هذه الاستراتيجيات العالمية أعدت في الفترة من عام ٢٠٠٨ إلى ٢٠١٤.
- المادة (٣٧) من اتفاقية مجلس أوربا للجريمة الإلكترونية تجيز مشاركة الدول غير الأعضاء في مجلس أوربا في معاهدات هذا الأخير، فمعاهدات مجلس أوربا المعنية والمسماة "المفتوحة" تجيز الانضمام إليها شريطة أن توجه الدعوة للقيام بذلك رسمياً من لدن لجنة الوزراء بمجلس أوربا، وتتبع حيثيات محددة في الأحكام الخاصة بكل معاهدة (أنظر الملحق رقم ٦)، وحتى الآن بلغ عدد الدول غير الأعضاء المنضمين لاتفاقية مجلس أوربا للجريمة الإلكترونية ٣٦ دولة ليس من بينها أي دولة في الشرق الأوسط.
- بلغ عدد مستخدمي الإنترنت في ٥ يناير ٢٠١٥ أكثر من ثلاثة مليار (٣,٥٤١,٣٦٥,٨٠٠) بنسبة ٤٠٪ من سكان العالم الذي وصل إلى (٧,٢٤٣,٧٨٤,١٢١) في ١ يوليو ٢٠١٤. وفي دول مجلس التعاون لدول الخليج العربية أفادت الإحصائيات في ١ يوليو ٢٠١٤ أن عدد مستخدمي الإنترنت في المملكة العربية السعودية (١٧,٣٩٧,١٧٩) بنسبة ٥٩,٢٤٪ من عدد السكان والترتيب العالمي للسعودية رقم (٣٠)، وعدد المستخدمين في دولة الإمارات العربية المتحدة (٨,٨٠٧,٢٢٦) بنسة ٩٣,٢٤٪ من عدد السكان، والترتيب العالمي رقم (٤٦)، وعدد مستخدمي الإنترنت في الكويت (٤,٠٢٢,٠١٠) بنسبة ٨٦,٨٦٪ من عدد السكان، والترتيب العالم رقم (٨٤)، وعدد مستخدمي الإنترنت في سلطنة عمان (٢,٥٨٤,٣١٦) بنسبة ٦٥,٨٢٪ من عدد السكان، والترتيب العالمي رقم (٨٩)، وفي دولة قطر عدد مستخدمي الإنترنت (٢,٢٦٧,٩١٦) بنسبة ـ ٪ من عدد السكان، والترتيب العالمي رقم (٩٣)، وفي مملكة البحرين عدد مستخدمي

الإنترنت (١,٢٩٧,٥٠٠) بنسبة ٩٦٪ من عدد السكان، والترتيب العالمي رقم (١١٥).

- تضاعف عدد مستخدمي الإنترنت عشر مرات في الفترة من ١٩٩٩- ٢٠١٣ وكان الوصول للمليار الأول من المستخدمين عام ٢٠٠٥ والمليار الثاني عام ٢٠١٠ والمليار الثالث في الربع الأخير من عام ٢٠١٤، وبالمقابل ارتفعت معدلات جرائم الإنترنت وقُدرت خسائر النشاطات الاقتصادية العالمية في عام ٢٠١٣ بأكثر من ٤٥٠ مليار دولار وبلغ عدد ضحايا الجريمة الإلكترونية ٥٥٦ مليون بواقع ١,٥ مليون ضحية في اليوم وبمعدل ١٨ ضحية كل ثانية.
- كشف تقرير نورتن سيمانتك لعام ٢٠١٢ أن خسائر دول مجلس التعاون الخليجي بسبب الجرائم الإلكترونية بلغت ٨٥٠ مليون دولار وفي عام ٢٠١٣ بلغت ٩٠٠ مليون دولار وكانت خسائر المملكة العربية السعودية وحدها ٥٢٧ مليون دولار حسب التقرير.
- في تقرير نورتن سيمانتك لعام ٢٠١٣ وردت كل من المملكة العربية السعودية ودولة الإمارات العربية المتحدة ضمن الـ ٢٤ الأولى في العالم التي تزاد فيها تهديدات الجريمة الإلكترونية المقلقة.
- وفقاً لتقرير المعهد الدولي للتنمية الإدارية لعام ٢٠١٢ احتلت دولة الإمارات العربية المتحدة المركز الأول في دول مجلس التعاون الخليجي والمرتبة الرابعة على مستوى العالم وكان ترتيبها عام ٢٠١١ رقم (٣٥)، ووفقاً لتقرير مؤشرات الأمن الإلكتروني لعام ٢٠١٣ احتلت سلطنة عمان المركز الأول.
- قام الاتحاد الدولي للاتصالات (ITU) A Blresearcg بتقييم أداء دول العالم في مجال الأمن السيبراني لعام ٢٠١٤ وجاء ترتيب دول الخليج العربي كالآتي من أصل ١٩٣دولة:

■ دولة الإمارات العربية المتحدة: الترتيب رقم (١٧) مشترك قبلها ٦٠ دولة.

■ مملكة البحرين: الترتيب رقم (١٩) مشترك قبلها ٧٥ دولة.

■ دولة الكويت: الترتيب العالمي رقم (٢٧) مشترك وهو المركز الثالث قبل الأخير ويأتي قبلها ١٦١ دولة.

■ سلطنة عمان: الترتيب العالمي رقم (٣) مشترك قبلها الولايات المتحدة الأمريكية في المركز

الأول وكندا في المركز الثاني واشتركت ثلاث دول في المركز الثالث هي استراليا وماليزيا وسلطنة عمان.

■ دولة قطر: الترتيب العالمي رقم (٨) مشترك قبلها ٢٣ دولة.

- شبكات التواصل الاجتماعي ألغت الحواجز الجغرافية والمكانية فهي عابرة للحدود بلا استئذان ويستطيع الفرد التواصل مع الآخرين بسهولة من أي مكان ولها استخدامات ايجابية ناجحة.
- تأكد وجود استخدامات سلبية لشبكات التواصل الاجتماعي مثل بث الافكار المتطرفة والهدامة وعرض المواد الإباحية والتشهير والمضايقة وبث الاشاعات والاحتيال والإبتزاز والتزوير وانتهاك الحقوق الخاصة والعامة والاستغلال الجنسي للأطفال, الإستلاب الثقافي واختلاط القيم الاخلاقية.
- تم تكثيف الجهود الدولية والإقليمية منذ العام ٢٠١٠ وعقدت عشرات المؤتمرات والندوات على نطاق العالم واسفرت عن توصيات كان من شأنها تعزيز جهود مكافحة الجريمة الإلكترونية.
- تم تأسيس مراكز تقنية وطنية وإقليمية ودولية لإعداد البرامج التنفيذية لحماية الأمن السيبراني ومن مكونات هذه المراكز " فرق الاستجابة لطوارئ الحاسب الآلي"

Computer Emergeny Response Team(CERT)

وتجدر الإشارة إلى أن أربعة من دول الخليج العربي أسست مراكز (CERT) وطنية حكومية وهي السعودية وسلطنة عمان والإمارات وقطر وفي الكويت أعُلن عن تأسيس هذا المركز في عام ٢٠١٢ ولكنه لم يباشر نشاطه حتى الآن وفي البحرين تم تأسيس المركز بواسطة القطاع الخاص.

- تم تأسيس المركز الإقليمي للأمن الإلكتروني للمنطقة العربية عام ٢٠١٤ ومقره مسقط, وله أهداف واستراتيجية ودور في تأهيل الكوادر وتطوير البرامج والحلول التقنية وتعزيز الجاهزية لمواجهة الجريمة الإلكترونية.

التوصيات:

- أن تتبنى الأمانة العامة لمجلس التعاون لدول الخليج العربية فكرة إعداد استراتيجية موحدة لمواجهة الجريمة الإلكترونية, تنطلق من رؤيتها وأهدافها ومبادئها الخطط والبرامج التنفيذية لمواجهة الجريمة الإلكترونية (مرفق استراتيجية مقترحة).
- تعزيز جهود التعاون الدولي بعقد المؤتمرات الدولية والإقليمية في دول مجلس التعاون الخليجي لمواجهة الجريمة الإلكترونية والمشاركة فيها في حالة عقدها في مكان آخر.
- دراسة الانضمام لاتفاقية مجلس أوربا للجريمة الإلكترونية (المفتوحة) بوصفها أول وأهم مبادرة عالمية في هذا المجال واستقطبت الكثير من دول العالم الراغبة في المشاركة في هذه الجهود الدولية.
- تبني إنشاء تحالف خليجي لحماية الأمن السيبراني أسوة بالتحالفات الدولية والإقليمية التي أشرنا إليها في متن البحث، واشتمل المطلب الثالث بالمبحث الخامس تصوراً كاملاً لمبررات هذا التحالف وضروراته وأهدافه وبرامجه التنفيذية وفوائده على مستوى القطاع العام والخاص.
- التأكد من أن تشريعات مكافحة الجريمة الإلكترونية مواكبة للتشريعات المقارنة العالمية وللتطورات في هذا الجانب وإقرار التدابير التشريعية وأنظمة العدالة الجنائية الفعالة.
- بناء القدرات في مجال تقنية المعلومات لرصد وتحليل التهديدات الأمنية المحتملة للجريمة الإلكترونية وآثارها والانذار المبكر باحتمالات وقوعها.
- بناء القدرات في مجال العدالة الجنائية (الشرطة والادعاء العام – القضاء) لتطوير التحقيقات الجنائية في مجال الجريمة الإلكترونية والأدلة الرقمية Digital Evidence وذلك بتوفير التدريب والتأهيل المناسب لرفع الكفاءة المهنية في هذا المجال الذي يواجه قصوراً نسبياً ملحوظاً.
- العمل مع الجهات المختصة لتكثيف التوعية الأمنية ضد الجريمة الإلكترونية في مراحل التعليم المختلفة من خلال محاضرات منهجية أو غير منهجية وإعداد منهاج لمؤسسات الشرطية التدريبية والتعليمية.

- تشجيع البحث والتطوير في مجال الحماية من الجريمة الإلكترونية ورصد انتهاكاتها وضبط أدلتها ومرتكبيها.
- بناء هياكل تنظيمية فعالة لتقييم وتقويم جاهزية الأمن السيبراني لمواجهة الجريمة الإلكترونية.
- اتخاذ التدابير اللازمة لحماية البنيات التحتية الحساسة وتعزيز صمودها في وجه الاختراقات والهجمات الإلكترونية.
- تكثيف التوعية الأمنية في مجال مكافحة الجريمة الإلكترونية بكافة الوسائل الممكنة.

وبالله التوفيق،،،

المراجع باللغة العربية

أولاً: المؤلفات:

١- د. أحمد الشربجي، د. وقائي بغدادي: حماية وتأمين الإنترنت التحدي القادم وأساليب المواجهة، سلسل العلوم والتكنولوجيا، الهيئة المصرية العامة للكتاب، القاهرة، ٢٠١٠.

٢- د. حسين بن سعيد الغافري. جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الانترنت . http://hussain-alghafri.blogspot.com/٢٠١١/٠٧/blog-post-٩٦٠٣.html ٢١/١٢/٢٠١٤ الساعة ١٨٥٣ .

٣- شمس الدين إبراهيم أحمد. وسائل مواجهة الاعتداءات على الحياة العربية. القاهرة ٢٠٠٥.

٤- د. المدرس المساعد. عادل يوسف عبدالنبي الشكري. الجريمة المعلوماتية وأزمة الشريعة الجزائية، مركز دراسات الكوفة، ٢٠٠٨.

٥- د. عبدالفتاح بيومي حجازي. مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي. دار الفكر الجامعي. الإسكندرية ٢٠٠٦.

٦- علي بن عبدالله عيسري: الآثار الأمنية لاستخدام الشباب للإنترنت ، مركز الدراسات والبحوث – جامعة نايف العربية للعلوم الأمنية، الطبعة الأولى ١٤٢٥هـ.

٧- د. محمد سامي الشوا. ثورة المعلومات وانعكاساتها على قانون العقوبات. مطابع الهيئة المصرية العامة للكتاب، مصر، ٢٠٠٣.

٨- محمد بن نصير محمد السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت. دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية: رسالة مقدمة الى كلية الدراسات العليا.

٩- مشعل عبدالله القدهي: المواقع الاباحية على شبكة الانترنت وأثرها على الفرد والمجتمع، مدينة الملك عبد العزيز للعلوم والتقنية.

١٠- د. نائلة عادل محمد فريد فودة . جرائم الحاسب الاقتصادية . دراسة نظرية تطبيقية ، دار النهضة العربية ، القاهرة ، ٢٠٠٤.

١١- الدكتور نبيل صلاح محمد العربي، أستاذ مساعد بكلية الاقتصاد والإدارة – جامعة القصيم دراسة بعنوان ''اقتصاديات الجرائم المعلوماتية.

١٢- يونس عرب: جرائم الكمبيوتر والإنترنت، منشورات اتحاد المصارف العربية، الاردن، ٢٠٠٢.

ثانياً: رسائل الدكتوراه والماجستير:

١- د. محمود العطا: دور التشريعات والإجـراءات الأمنية في التصدي للإجرام المعلوماتي، رسالة دكتوراه (بحث غير منشور)، جامعة الرباط الوطني، الخرطوم، السودان ٢٠٠٧.

٢- عبدالله بن أحمد الغامدي: تردد المراهقين على مقاهي الانترنت وعلاقته ببعض المشكلات لدى عينة من طلاب المرحلة الثانوية بمكة المكرمة ، رسالة الماجستير – جامعة أم القرى، ١٤٢٩هـ .

٣- عبدالله حسين آل حجراف القحطاني . تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية . دراسة تطبيقية في هيئة التحقيق والادعاء العام بمدينة الرياض . رسالة ماجستير . الرياض . ١٤٣٥ . ٢٠١٤م. http://repository.nauss.edu.sa ٣٠/١٢/٢٠١٤ الوقت ١٧٠٠.

ثالثاً: البحوث المقدمة للمؤتمرات:

١- د. محمد الامين البشري . التحقيق في جرائم الحاسب الآلي . بحث مقدم إلى مؤتمرات القانون والكمبيوتر والانترنت . كلية الحقوق والشريعة . جامعة الامارات ٢١ . مايو ٢٠٠٥.

٢- د. محمد عبدالرحيم سلطان العلماء . جرائم الإنترنت والاحتساب عليها . بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت . جامعة الامارات . مايو ٢٠٠٥.

رابعاً: الدوريات:

١- فايز الشمري: استخدامات شبكة الإنترنت في الإعلام العربي ، مجلة البحوث الأمنية كلية الملك فهد العدد التاسع عشر شعبان ١٤٢٢هـ .

٢- منى شاكر فراج العبسلي: مقال بعنوان تأثير الجريمة الالكترونية على النواحي الاقتصادية . ://www.shatharat.net/vb/showthread.phpptth ٢٠١٤/١٢/٢٤ الوقت ١٧٢٧ .

المراجع باللغة الإنجليزية

References

Organizations and Specialized Studies Centers;

Studies and Report's;

أولاً: منظمات ومراكز أبحاث متخصصة: دراسات وتقارير:

Computer Emergency Response Team (CERT) Created in1988 at Carnegie Mellon University .USA

1- Computer Emerqency Response Team (ae CERT) United Arab States
2- Council of Europe (committee of Ministers) 1989.
3- Council of Europe- Explanatory Report to the Convention on Cybercrime , (ETS No.185) Introduction, No. 111, The Convention , p.3.
4- Michael E. Porter, Mark R-Kramer, Creating Shared, Value, Harvard Business Review, January-Feb,2011 edition.
5- Net Losses; Estimating the Global cost of Cybercrime, Economic Impact of, Cybercrime11. Report Summary. Intel Security. 2014. www.macfee.com
6- National Information Safety Center (oman) Computer Emergency Response Team (CERT- om).
7- Number of Internet Users (2014) Internet Live stats, www.inernetlivestats internet- users.
8- Norton Cybercrime Report September 2012.
9- Qater Cybercrine Emerqency Response Team (Q- CERT) National Information Security Center.
10- Saudi Arabia Computer Emerqency Response Team (CERT- SA).
11- Supreme Council of Information and Communication Technology (ict QATR)
12- WAVEFRONT. Consulting Group. Certified Information Security Consults . Brief History of Cybercrime. 2012 ; www.warefrontcg.com.

ثانياً: وثائق وتوصيات المؤتمرات والندوات:

1. World Summit Information Society, Swiss, Geneva, 10-14 May 2010.
2. G-8 Information Centre, Deauville Summit, France 26 May 2011.
3. http://www.g8.utoronto.ca/summit/2011/deaurille/2011-lmternet-en-html
4. CSEC 2014 Cyber security Summit, Kingdom of Bahrain, October 20-22,2014.
5. Cyber Security Summit 2014,Minneapolis,Minnesta, USA .October 21-22,2014.
6. Cyber Security Conference, New York University Technology, 18 Sep.2014
7. Developing Police Force Cybercrime investigation Skills and Techniques-Digital Forensics Technology and Comprehensive Cybercrime Strategies.

8. GLACY/Cyber crime @EAP:/International Workshop on mainstreaming judicial training on Cybercrime and electronic evidence, Bucharest,Romania,2-3June 2014.
9. European Cybercrime Training and Education Group (ECTEG), Cofi Annan international Peace Keeping Training Centre in Accra, Ghana, from 18 to 21 March2014.
10. GLACY Conference; Getting started ,24-27March 2014 Dakar , Senegal.
11. Global Cyber security Conference in Abu Dhabi: National and Corporate Threats, Protection, And Education, March 25,2014.

ثالثاً: مواقع إلكترونية:

1- www.Meed.com/sector/Markets/ commodities/ 28 May 2014
2- www.Alarabiya .net/ar/techonlgy. 31 Jan 2013 موقع العربية
3- www.Jlegt- com. 28 Jan 2014 cost of cyber crime study repent. H.P Enterprise security.
4- www.artnews.com/26 June 2013
5- Cyber Threat Map. 28 May 2014 AR- Wikipedia- org. Indie-
6- Kasper Sky.com/news=9074/24 sepal- 2014
7- www.nxme.net /information
8- جريدة الاتحاد الإماراتية، بتاريخ 23 فبراير 2013.
9- Symantec- Internet Security Threats.
10- http://www.alukah.net/culture/0/59302
11- http://www.alukah.net/publications-competitions/0/404
12- http://lljk599.blogspot.com/2014/04/blog-post-6251.html
13- http://www.almaaref.org/books/contentsimages/books/zad-almobalegh /zad -alrahma-fe-shahr-alla h/page/lesson14.htm
14- وأنظر الملحق رقم (2)، والموقع الإلكتروني التالي: http://www.alriyadh.com/980890
15- http://www.kolalwatn.net/news136120
16- http://www.mbrsg.ae/getattachment/9cea0fcc-9e43-4fba-9f47-ea6d9d16ca8c/Arab-Social-Media-Outlook 2014.aspx
17- http://arabic.arabianbusiness.com/politicseconomics/society/2014/jun/25/364833/#.VK5jWujTHAw
18- أنظر الموقع الإلكتروني السابق، www.cert.org/incident
19- لمزيد من المعلومات حول المؤتمر أنظر الموقع الاليكتروني التالي: fbi.gov./news/stories/20 www.
20- أنظر موقع موسوعة ويكيبيديا الاليكتروني : http://wikcfp.com/cfp/servlet/even
21- أنظر الموقع الإلكتروني السابق، www.cert.org/incident

22- (المصدر: الموقع الإلكتروني للاتحاد الدولي للاتصالات ITU :(www.itu.int/en/ITU-D/cybersecrity/pages/GCI-aspx

23- المصدر: الموقع الإلكتروني للمركز الوطني للسلامة المعلوماتية بسلطنة عمان: www.cert.gov.om/about وأنظر كذلك قائمة مراكز CERT.... حول العالم، ملحق رقم

24- http://www.go-gulf.com/blog/cybe.

25- AR- Wikipedia- org. Indie- Cybercrime. Kasper. com.23/9/2014 مستخرجة بتاريخ

26- ww.Meed.com/sector/Markets/ commodities/ 28 May 2014

27- أنظر موقع موسوعة ويكيبيديا الاليكتروني : http://wikcfp.com/cfp/servlet/even

28- www.reuters. Com, article/ 17 May 2013.. وكالة رويتر

29- AR- Wilkipedia, org. India- Cybercrime, Kasper,com. .23/9/2014 مستخرجة بتاريخ

30- www. Meed, com/ sector/ Markets,28 May 2014.

31- www. Alarabiya, net/ ar/ techonlgy, 31 Jan 2013. موقع العربية

32- الموقع الإلكتروني للمركز الوطني للسلامة المعلوماتية بسلطنة عمان: www.cert.gov.om/about

ملحق رقم (١)

استراتيجية موحدة لمواجهة الجريمة افلكترونية

في دول مجلس التعاون لدول الخليج العربية

من أ ــ م

مقدمة:

حققت البشرية فوائد عظيمة جداً ونقلة نوعية تاريخية نتيجة للثورة التكنولوجية الهائلة في مجال تقنية المعلومات والاتصالات وتطبيقات الحاسب الآلي وشبكة الإنترنت ، حتى أصبح الاعتماد على هذه التقنيات أحد أبرز أساسيات الحياة المعاصرة في كافة المجالات الاقتصادية والاجتماعية والسياسية والأمنية والدفاع، بما تشمله من تفاصيل، وعلى مستوى الأفراد. وحقق استخدام هذه التقنيات نهضة كبرى غير مسبوقة وازدهارا علمياً واقتصادياً وصناعياً وطبياً وهندسياً... إلخ(١٦٦)، حتى بلغت مبيعات الحاسب الآلي في يوم واحد هو ٣٠ نوفمبر ٢٠١٤ الساعة ٢١:٢٨ : ٦٦٥ ألف ٦٢٥ وجهاز، مما جعل معلومات وبيانات وأحداث العالم بين يدى الأفراد في هاتف ذكي محمول، وقد رصدت الإحصائيات مبيعات الهواتف الذكية المحمولة يوم ٣٠ نوفمبر ٢٠١٤ الساعة ٢٠:٣٠ فبلغت ٣,٦٠٥,٠٠٠ هاتف وقد بلغ عدد مستخدمي الإنترنت في يوليو ٢٠١٤: ٢,٩٢٥,٢٤٩,٣٥٥ بنسبة نمو ٧٩٪ من السنة السابقة وبنسبة ٤٠,٤٪ من عدد سكان العالم البالغ ٧٢٤٣,٧٨٤,١٢١ في نفس التاريخ. وبلغ عدد مستخدمي الإنترنت في دول الخليج العربي ٣٥,٢٩٩,٩١٧ نسمة بنسبة ٧٠,٨٪ من عدد السكان البالغ ٤٩,٨٣٢,٩٤٢ في ١ يوليو ٢٠١٤.(١٦٧)

تبعاً لذلك، فإن الجريمة الإلكترونية بوصفها عابرة للحدود ويمكن ارتكابها من أي مكان في العالم مع صعوبة كشف أدلتها، تسارع نمو معدلاتها وتضاعفت أضرارها وخسائرها المادية العالمية التي قدرت بـ ٤٥٠ مليار دولار لعام ٢٠١٣، وشهدت منطقة الخليج العربي في عام ٢٠١٢هجمات الإلكترونية على منشآت شركة أرامكو السعودية وعلى شركة رأس غاز القطرية، وفي مايو عام ٢٠١٣ أُطلقت هجمات على مواقع إلكترونية حكومية في المملكة العربية السعودية أدت إلى تعطيل موقع وزارة الداخلية مؤقتاً.(١٦٨)وقدرت خسائر النشاطات التجارية في دولة الإمارات العربية المتحدة بسبب الهجمات الإلكترونية بـ ٤٢٢ مليون دولار عام ٢٠١٢.(١٦٩)

١٦٦ Number of Internet Users (2014) Internet Live Stats www.internet live stats /Internet- users

١٦٧ المصدر: Number of IntemetUsers (2014) – Internet Live Stats

www.Interretlivestats.com /internet-users.

١٦٨ أنظر الموقع التالي: -http://www.reuters-com/article/2013/05/17us-saudi-cyber-idUSBRE94G oly2013-50-17./17

١٦٩ أنظر تقرير شركة نورتن لعام Norton Cybercrime Report. September 2012:2012

ولازالت الجريمة الإلكترونية تهدد كل مقدرات المجتمع الدولي على صعيد القطاع العام والخاص وعلى مستوى الأفراد، والتوجه الدولي هو التكاتف والتحالف والتعاون الدولي والإقليمي لمواجهة تهديدات ومخاطر الجريمة الإلكترونية، حيث لا تستطيع دولة بمفردها أن تواجه مشكلة عالمية بالغة التعقيدكهذه ، من هذا المنطلق أصبح لابد من أن تتفق دول مجلس التعاون لدول الخليج العرية كغيرها من دول العالم التي عقدتالاتفاقيات والتحالفات الدولية والإقليمية على رؤية وأهداف محددة وإدراك وفهم عميق للتهديدات واستصحابلمبادئ أساسية ترسم خارطة الطريق لاستراتيجية تعزز الصمود في مواجهة الجريمة الإلكترونية وتحد من ارتكابها وخسائرها وتكشف أدلتها وتضبط مرتكبيها وتعزز الثقة في أنظمة تقنية المعلومات وتطبيقاتها وتحقق الأمن السيبراني في كافة تعاملات القطاع العام والخاص والأفراد من خلال التدابير التشريعية وأنظمة العدالة الجنائية الفعالة الهياكل التنظيمية، بناء القدرات، حماية البنيات التحتية الحساسة والتعاون الدولي.

وتجدر الإشارة إلى أن هناك فهماً دولياً مشتركاً للأهداف والمبادئ الاستراتيجية لمواجهة الجريمة الإلكترونية وحماية الأمن السيبراني، وبناء على ذلك، تم استخلاص مبادئ ومفاهيم هذه الاستراتيجية من استراتيجيات عشرة دول منها خمسة دول – أوروبية رئيسية إضافة – إلى الولايات المتحدة الأمريكية وكندا واستراليا واليابان والهند، فضلا عن الاستعانة في نطاق محدود جداً بمشروع الاستراتيجية الاستراتيجية العربية لمواجهة الجريمة الإلكترونية الصادرة عن مجلس وزراء الداخلية العرب عام ٢٠١١.

وبالله التوفيق.

التهديدات:

١. هناك طرق عديدة للحصول على المعلومات عبر الفضاء السيبراني، حيث يمكن للمهاجمين استغلال نقاط الضعف في أنظمة الحاسب الآلي software and hardware ويمكنهم استغلال الثغرات في أنظمة أمن المعلومات بخداع مستخدمي الإنترنت بفتح رسائل بريد إلكتروني مصابة أو زيارة مواقع إلكترونية مشبوهة تصيب أجهزتهم بالبرمجيات الخبيثة، ويستهدف المهاجمون بصفة خاصة الأشخاص الذين يفشلون في اتباع قواعد الأمن السيبراني مثل تغيير كلمة السر Password من وقت لآخر والحرص على تحميل وتحديث برامج الحماية ضد الفيروسات بطريقة منتظمة واستخدام إنترنت لاسلكية محمية فقط.[١٧٠]

٢. على الرغم من أن بعض أدوات وتقنيات الهجوم هي أكثر تكلفة وتعقيداً من غيرها، تشترك معظم الهجمات الإلكترونية في أربع خصائص وترجع بعض الأسباب لشعبيتها المتزايدة وغالباً تكون كما يلي:

أ- كثير من الأدوات التقنية المستخدمة في الهجوم تباع بأسعار غير مكلفة أو يمكن الحصول عليها بالمجان من الإنترنت.

ب-المهاجمون ذوى المهارات الأولية يمكنهم إحداث أضرار كبيرة.

ج-الهجمات الصغيرة قد تكون فعالة وتسبب تدميراً ممتداً.

د-إحساس المهاجم بقلة المخاطر لصعوبة كشفه بسبب إخفاء جريمته من خلال شبكة معقدةمن الحواسيب الآلية واستغلال الثغراتفي الأنظمة القانونية المحلية والعالمية.[١٧١]

٣. يجب التعرف على مخاطر الأمن السيبراني وتقييمها وتحليلها في مرحلة مبكرة من أجل تقليل المخاطر، وعدم منع استخدام التدابير اللازمة لمواجهتها بالتعاون مع كل الشركاء في القطاع العام والخاص والدوائر السياسية والمجتمع.

٤. تهديد البنيات التحتية الحساسة قد يشمل مؤسسات القطاع العام والخاص، وعليه فإن صمود البنيات التحتية الحساسة للهجمات الإلكترونية يتطلب زيادة تعاون كل الجهات المختصة وذات الصلة ببرمجة وتشغيل وحماية أنظمة تقنية المعلومات لحمايتها وتمكينها من الصمود.

٥. التأكيد على توفر المتطلبات اللازمة للحد من المخاطر وبصفة خاصة الجريمة الإلكترونية،

---

١٧٠ أنظر استراتيجية كندا للأمن السيبراني لعام ٢٠١٠، فهم تهديدات الأمن السيبراني، ص٤.

Canada›s Cyber Scanty Stiategy,2010 ‹Understanding Cyber Threats›,p.4

١٧١ أنظر المرجع السابق.

التجسس الإلكتروني Cyber espionage، والتخريب الإلكتروني Cyber sabotage.[١٧٢]

٦. يجب الإقرار بأن التطور المتلاحق للشبكات تنتج عنه في كل مرة تحديات جديدة للأمن القومي والاقتصادي وللمجتمع الدولي وتتمثل هذه التحديات فيما يلي:

أ- الكوارث الطبيعية.

ب- الحوادث.

ج- تخريب الكوابل، والخوادم Servers والشبكات اللاسلكية في الأرض أو تحت الأرض.

٧. التحديات الفنية قد تتحول إلى معوق لأداء شبكة الإنترنت، فإغلاق موقع معين website في بلد ما قد يؤدى إلى تعويق أكبر حجماً في الشبكة الدولية.

٨. عمليات الابتزاز والاحتيال وسرقة الهويات والاستغلال واستغلال الأطفال، من شأنها أن تهدد ثقة مستخدمي الإنترنت في التعاملات المالية والاقتصادية عبر الإنترنت، وكذلك تقلل الثقة في شبكات التواصل الاجتماعي بل في السلامة الشخصية.

٩. سرقة حقوق الملكية الفكرية تهدد المنافسة المشروعة التي يقودها الابداع.

١٠. هذه التهديدات عابرة للحدود وقليلة التكلفة للوصول إلى الفضاء السيبراني فضلاً عن إمكانية إخفاء هوية الجاني.

١١. تهديدات الأمن السيبراني من شأنها أن تشكل خطورة على السلم والأمن الدوليين بصورة أوسع مثلما تنتشر النزاعات التقليدية في الفضاء السيبراني.[١٧٣]

١٢. التهديدات الموجهة إلى الدولة تشمل الآتي:

أ- استهداف خدمات الدولة عبر الإنترنت للجمهور (أفراد وقطاع خاص)، من أجل الكسب المالي.

ب- جمع بيانات الأفراد من السجلات الرسمية للدولة.

ج- زيادة وانسياب خدمات الدولة للجمهور عبر الإنترنت تتيح الفرص لمجرمي الإنترنت.

د- القيام بعمليات الاحتيال بتقديم الطلبات المزورة والهويات المسروقة للحصول على خدمات أو ميزات بطرق غير مشروعة.[١٧٤]

---

١٧٢ أنظر: استراتيجية سويسرا الوطنية للحماية ضد المخاطر السيبرانية، ٢٠١٢، البنود ٣-٥، ص٢٨.
National Strategic for the Protection of Switzerland against Cyber risk,2012.p-28

١٧٣ أنظر الاستراتيجية الأمريكية الدولية للأمن السيبراني، مايو ٢٠١١، ص٤:
US. International Strategy for Cyberspace, Recognizing the challenges,p4.

١٧٤ أنظر استراتيجية المملكة المتحدة للجريمة الإلكترونية لعام ٢٠١٠ (The Threat to Government) ، ص16.

١٣. **حماية الأطفال من مخاطر الإنترنت:** يستخدم الأطفال الإنترنت بشكل مكثف لأغراض مختلفة ومنها على سبيل المثال استخدام مواقع التواصل الاجتماعي، وألعاب التسلية، وللبحث عن المعلومات واعداد المشروعات البحثية المدرسية، وبالتالي يستغل من يرغبون في تسبب الاذى للأطفال وجودهم المكثف على الإنترنت.

تتمثل مخاطر الإنترنت بالنسبة للأطفال في التحرش والاستغلال الجنسي بوسائل وأغراض متعددة ومنها ما يلي:

أ- استهداف الأطفال والمراهقين أثناء استخدام الإنترنت وبصفة خاصة ارسال الرسائل والدردشة وفي مواقع التواصل الاجتماعي.

ب- بعض المتورطين بالتحرش والاستغلال الجنسي للأطفال يصورون مشاهدة لمارساتهم أو ممارسات غيرهم ويتبادلونها عبر شبكات الإنترنت مع من يرغب من الأشخاص أو مع الذين يهوون جمع هذا النوع من المشاهد المصورة.

ج- الأشخاص الذين يستخدمون الإنترنت للتعرف على أفضل الاماكن في العالم للاستغلال الجنسي للأطفال والمراهقين أو الأشخاص الذين يستخدمون الإنترنت لأغراء وإخضاع الأطفال لبعض أنواع الاستغلال.

د- الأشخاص الذين يشكلون خطراً على استخدام الأطفال للإنترنت قد يرغبون في الأولاد أو البنات أو في الأثنين معاً.[١٧٥]

١٤. استخدام الإنترنت لنشر الأفكار المتطرفة والهدامة والدعوة للإرهاب وتمويل الإرهاب وعمليات الأموال.

١٥. اختراق المنظمات الإرهابية للمواقع الحساسة للأجهزة الأمنية والدفاع ودوائر صنع القرار.[١٧٦]

---

١٧٥ أنظر استراتيجية المملكة المتحدة للجريمة الإلكترونية، مرجع سابق، ص١٢:
UK .Cyber Crime Stiategy,2010.Threat, to Children,p.12.

١٧٦ في واقعة حديثة أثناء إعداد هذه الاستراتيجية، أذاعت قناة الجزيرة الإخبارية في نشرة حصاد اليوم الإخباري يوم ٢٠١٥/١/١٢ أن قراصنة مؤيدون لتنظيم الدولة الإسلامية تمكنوا من اختراق حسابات القيادة الأمريكية الوسطى على (تويتر) و (يوتيوب) وقاموا بنشر أسماء جنرالات وعناوينهم ووثائق أمريكية وأن الاختراق تم باللغات الإنجليزية والعربية والروسية، مساعد وزير الدفاع الاسبق (لاري كورب) أكد الواقعة في مقابلة مع قناة الجزيرة وقال أن تنظيم الدولة الإسلامية له مقدرات لم تكن معروفة، واعترفت واشنطن بالاختراق ووصفته بأنه (مقلق ولكنه لا يشكل تهديداً أمنياً). وأعلن الرئيس الأمريكي باراك أوباما في مؤتمر صحفي يوم الجمعة ٢٠١٥/١/١٦ عن اتفاقه مع رئيس الوزراء البريطاني على تشكيل «خلية إلكترونية» لمكافحة الإرهاب الدولي، وأكد على ضرورة تفعيل التعاون الدولي في مجال تقنية المعلومات والاتصالات لتعزيز جهود المكافحة.

الرؤية:

التمتع بأقصى درجات الأمن السيبراني في مرافق القطاع العام والخاص والأفراد وجعل دول مجلس التعاون لدول الخليج العربية هدفاً صعباً للجريمة الإلكترونية.[١٧٧]

الأهداف:

يتم تحقيق الرؤية من خلال الأهداف التالية:

1- أن تكون دول مجلس التعاون لدول الخليج العربية من أكثر الاماكن أمناً في العالم للقيام بالأعمال التجارية وغيرها في الفضاء السيبراني تشجيعاً للاستثمار وتعزيزاً للازدهار الاقتصادي.

2- أن تكون دول مجلس التعاون لدول الخليج العربية أكثر صموداً في مواجهة الهجمات الإلكترونية وأقدر على حماية مصالح شعوبها في الفضاء الإلكتروني.

3- الاسهام مع المجتمع الدولي في إيجاد فضاء إلكتروني Cyberspace يتمتع بالانفتاح والحيوية والاستخدام الآمن، ويدعم التواصل بين أفراد المجتمعات حول العالم.[١٧٨]

4- تعزيز الثقة في أنظمة تقنية المعلومات (IT InformationTechnology) .

5- تنمية وتطوير القدرات وتدريب وتأهيل الكفاءات في كافة المجالات ذات الصلة.

6- مواجهة الجريمة الإلكترونية بالتدابير الفعالة في مجالات العدالة الجنائية بسن القوانين الملائمة وتنمية القدرات ورفع الكفاءة في مجالات التحقيق وتعزيز سلطات الادعاء العام.

7- تعزيز التعاون الدولي في مجال الجريمة الإلكترونية والأمن السيبراني بالمشاركة الفاعلة في الجهود الدولية والإقليمية.[١٧٩]

---

١٧٧ الرؤية: في غالبية الاستراتيجيات التي اطلعنا عليها تكون مختصرة ومعبرة، وأحياناً تتضمن عدة عناصر، أنظر أمثلة فيالاستراتيجيات التالية:

-UnitedKingdomCybercrime Strategy,2010.The Threat to Government, Vison, No4, 1.p27,United Kingdom Cybercrime Strategy, 2011- 2015 The Government Response,Vision for 2015,p.21.
- Australia National plan to Combat Cybercrime.2013. Vision,p8.
- Japan Cyber Security Strategy, June 2013, Vision, p.19.
- India National Cyber Security Policy, 2013, Vision, No1.p.3.

١٧٨ اقتبسنا مفهوم الأهداف (١، ٢، ٣) من أهداف استراتيجية المملكة المتحدة للأمن السيبراني، ٢٠١١- ٢٠١٥، مرجع سابق، ص٣٦-٤٢. لأنها ذات دلالات استراتيجية عميقة وطموح مشروع يشكل محور الأهداف الرئيسية لحماية الأمن السيبراني ومواجهة الجريمة الإلكترونية.

١٧٩ أنظر استراتيجية اليابان للأمن السيبراني لعام ٢٠١٣، مرجع سابق، ص١٩. وأنظر كذلك: السياسة الهندية للأمن السيبراني، مرجع سابق، ص٣٢-٤٠ India National Cyber Security Policy, 2013, Vision, No1.p.3.

وأنظر كذلك: مشروع الاستراتيجية العربية لمواجهة الجريمة الإلكترونية، الذي أصدرته مجلس وزراء الداخلية العرب عام ٢٠١1، ويلاحظ أن تعزيز التعاون الدولي عنصر مشترك في كل الاستراتيجيات العالمية.

المبادئ الأساسية للاستراتيجية:

يرتكز تحقيق أهداف الاستراتيجية على مجموعة من المبادئ الأساسية كما يلي:

١. التدابير التشريعية وأنظمة العدالة الجنائية الفعالة.
٢. الهياكل التنظيمية.
٣. بناء القدرات في كافة المجالات ذات الصلة.
٤. حماية البنيات التحتية الحساسة.
٥. التعاون الدولي.[١٨٠]

وسائل وآليات تفعيل المبادئ الأساسية للاستراتيجية:

المبدأ الأول: إقرار التدابير التشريعية وأنظمة العدالة الجنائية الفعالة:

يجب أن تكفل التشريعات الاعتراف بالحقوق التالية:

١. كفالة سائر الحقوق والمصالح القانونية ذات الصلة بالمعلومات وتقنية المعلومات وتطبيقاتها بإصدار التشريعات الملائمة التي تحقق التوازن بين حرية وخصوصية استخدام الإنترنت وبين مصلحة المجتمع في محاربة الجريمة الإلكترونية وكشف المخططات والتهديدات وملاحقة الجناة.
٢. الحق في الوصول إلى المعلومات بالطرق المشروعة ووفقاً للضوابط والبروتوكولات المنظمة لذلك.
٣. كفالة أمن المعلومات على مستوى القطاع العام والخاص والأفراد.
٤. حماية حقوق الملكية الفكرية.
٥. حماية الحق في حرية الحياة الخاصة للأفراد بحماية بياناتهم ومعلوماتهم وحماية خصوصية معلومات وبيانات مؤسسات القطاع العام والخاص.
٦. الحق في الإدارة الرشيدة للمعلومات والمعرفة عبر كفالة حق مالكي المعلومات (بأشكالها المختلفة) المصنفة أو الخاصة بنشاطهم الاستثماري أو التجاري وإدارتهم للمعلومات والمعرفة التي تمثل رأس المال الفعلي لمشروعاتهم.[١٨١]

---

١٨٠ المبادئ من (١-٥) تعد عناصر مشتركة في غالبية الاستراتيجيات أعدتها لجنة خبراء رفيعة المستوى Global Cyber Security (GCA) في عام 2007 بتكليف من منظمة (The High Level Experts Group (HLEG AgendaAgenda التابعة للاتحاد الدولي للاتصالات (ITU)، وبما أن كل استراتيجيات الأمن السيبراني والجريمة الإلكترونية قد تم إعدادها اعتباراً من عام 2008 والأعوام التالية، فقد أصبحت هذه المبادئ عناصر مشتركة في غالبية الاستراتيجيات وهي:

1- Technical and Procedural Measures-2 Legal Measure
3- Capacity Building-4 OrganizationalStructures
5- International Cooperation

أنظر تقرير لجنة الخبراء رفيعة المستوى المشار إليها في الموقع الإلكتروني لـ Global Cyber Security Amends (GCA)

١٨١ تم اقتباس مضمون بعض الحقوق المشار إليها في المبدأ الأول، البنود (١-٦) من مشروع الاستراتيجية العربية لمواجهة الجريمة الإلكترونية لعام ٢٠١١، الذي أعدته الأمانة العامة لمجلس وزراء الداخلية العرب ولم يجاز حتى الآن .

٧. إصدار التشريعات التي تكفل نظام عدالة جنائية فعال في المجالات الأساسية التالية:

أ- مواكبة التشريعات للتطورات الملاحقة في تقنية المعلومات والأساليب التقنية المستجدة لارتكاب الجرائم.

ب-فرض عقوبات تحقق الردع الملائم وتعكس مدى خطورة الجرائم الإلكترونية بأنواعها المختلفة.

ج-إعادة النظر في نظام الإجراءات الجنائية وقواعد الأدلة الجنائية بشأن الجرائم الإلكترونية وابتكار أنظمة ملائمة وتُشرَّع قواعد التعامل مع الدليل الرقمي.

د-تأهيل منسوبي السلطات المختصة في الشرطة والادعاء العام والهيئة القضائية بالمعارف والقواعد اللازمة للتعامل مع الدليل الرقمي.[١٨٢]

هـ-إتباع سياسة تشريعية تستجيب بالكامل للاتفاقيات والمعاهدات الدولية والإقليمية ذات الصلة.

و-تركيز التشريعات على مكافحة النشاطات غير المشروعة وليس التركيز على سياسات تقيد استخدام الإنترنت أو الوصول إلى محتوياتها.

ز-تجريم استغلال الإنترنت للتخطيط للعمليات الإرهابية والحصول على التمويل وتدبير الهجمات الإلكترونية.[١٨٣]

ح-إيجاد قاموس لمصطلحات الأمن السيبراني.[١٨٤]

المبدأ الثاني: هياكل تنظيمية فعالة:

تتولى الهياكل التنظيمية الفعالة تقييم وتقويم جاهزية الأمن السيبراني ويتم ذلك من خلال المهام والإجراءات التالية:

---

١٨٢ هذا البند (٧) من المبدأ الأول عنصر أساسي ومشترك في كافة الاستراتيجيات العالمية، وتم اقتباس مضمون الفقرات (أ، ب، ج، د) من استراتيجية استراليا لمواجهة الجريمة الإلكترونية لعام ٢٠١٣، مرجع سابق، تحت العنوان التالي:
KEY PRIORITY-Ensuring The Criminal Justice Framework is Effective
أنظر كذلك استراتيجية سويسرا لمواجهة الجريمة الإلكترونية لعام ٢٠١٢، ص٢٣-٢٦ وتتضمن أمثلة لتشريعات مواجهة الجريمة الإلكترونية.عنوان الاستراتيجية: National Strategy for Protection of Switzerland against Cyber risks.2012.

١٨٣ أنظر هذا المفهوم في استراتيجية الولايات المتحدة الأمريكية للفضاء السيبراني، مايو ٢٠١١، ص١٩-٢٠
US. International Strategy for Cyberspace, Recognizing the challenges,p.19-20.
ومنها تم اقتباس مضمون الفقرات (هـ، و، ز) بالبند (٧) بالمبدأ الأول.

١٨٤ أنظر استراتيجية تركيا للأمن السيبراني ٢١٣- ٢٠١٤، ص٢٣-٢٧.
Republic of Turkey National Cyber Security Strategy and 2013-2014 Action Plan,Carrying out Legislative Activities, No.2. CreatingDictionary of Cyber Security Terms,p.23.

1- تعيين منسق قومي للأمن السيبراني أو إنشاء مجلس قومي للأمن السيبراني تكون مراكز الاستجابة لطوارئ الحاسب الآلي الوطنية (CERT) أحد مكوناته، ويحدد قرار التشكيل العضوية والاختصاصات.[١٨٥]

2- التعرف على أفضل البرامج والمواد المطورة التي تلبى حاجات مستخدمي الإنترنت.

3- تعزيز برامج حماية تقنية المعلومات والاتصالات.

4- تقييم وتحليل المخاطر وإتباع الطرق المعتمدة في إدارة مخاطر تقنية المعلومات والاتصالات.

5- رعاية ومتابعة وتطوير الأساليب المتعلقة بفرق الاستجابة لحوادث الحاسب الآلي ومدى مقدرات مواجهة التهديدات المتغيرة لتقنية المعلومات والاتصالات وذلك بالتعاون مع المنظمات المختصة.

6- تحديد طرق دعم جاهزية الطوارئ واستمرارية التخطيط.

7- عقد ورش العمل المحلية والإقليمية وسمنارات تعزيز المهارات والقدرات.

8- أن تكون معايير أمن المعلومات وفقاً لما أقرته المنظمة العالمية للمقاييس (ISO) بشأن إدارة وحماية أنظمة أمن المعلومات.

9- تطوير وتبنى سياسات واستراتيجيات قومية للأمن السيبراني وتسخير الموارد اللازمة لتنفيذها بدعم القطاع العام والخاص والمؤسسات الأكاديمية والمجتمع المدني.[١٨٦]

10- التنسيق بين السلطات الأمنية المختصة وآلية التعامل الاستراتيجي المشار إليها في البند [١] ووزارة العدل ومؤسسات تقنية المعلومات لإيجاد وتطوير معايير لتداول البيانات بحيث يراعى فيها كل الأفراد والجهات الأخرى التي يبدها بيانات شخصية للأفراد متطلبات التعامل مع هذه البيانات.[١٨٧]

11- الشراكة في مسؤولية حماية الأمن السيبراني بين الجهات الحكومية المختصة.

المبدأ الثالث: بناء القدرات في كافة المجالات ذات الصلة بالجريمة الإلكترونية والأمن السيبراني:

إن طبيعة الجرائم الإلكترونية من حيث سرعة ارتكابها وعبورها للحدود الدولية تفرض

---

١٨٥ أنظر استراتيجية المملكة المتحدة للأمن السيبراني، مرجع سابق، ويحدد قرار التشكيل العضوية والاختصاصات.

١٨٦ أنظر المرجع السابق: ITU Global Cyber SecurityAgenda,OrganizationalStructures, P.12.

وفي مفهوم مقارب أنظر كذلك الاستراتيجية الأمريكية للفضاء السيبراني لعام ٢٠١٣، مرجع سابق، ص٢١-٢٢.
US. International Strategy for Cyberspace. Internet Governess: Promoting Effective and Inclusive Structure›s. p21-22

١٨٧ أنظر استراتيجية المملكة المتحدة للجريمة الإلكترونية لعام ٢٠١٠، مرجع سابقن ص١٩، بند٨٣.

تحديات جديدة على السلطات التشريعية وسلطات انفاذ القانون، ومن أجل إيجاد رد الفعل المتحمل القوى في مواجهة الجريمة الإلكترونية، أصبحت الحاجة ماسة لتجاوز الطرق التقليدية لنشاطات انفاذ القانون واكتشاف خيارات جديدة للكشف عن الجرائم الإلكترونية ومنعها أو إعاقة هذه النشاطات الإجرامية عبر شبكة الإنترنت.

بناء على ما تقدم، يجب أن نهدف إلى التأكيد بأن السلطات المختصة بمواجهة الجريمة الإلكترونية تمتلك المقدرات والقدرات الفعالة للاستجابة للجريمة الإلكترونية ومواجهة كل العوائق التي تؤثر على التعاون في الاستجابة للجريمة الإلكترونية محليا وعالمياً.[١٨٨]

لتحقيق ما تقدم، يجب التركيز على:

١. تحسين التنسيق للاستجابة ومواجهة الثغرات المحددة في مجال المقدرات والقدرات في كافة المجالات ذات الصلة بالجريمة الإلكترونية والأمن السيبراني.
٢. تأهيل وتدريب الكوادر المختصة في القطاع العام والخاص لبناء القدرات ودعم حاجة الأمة للأمن السيبراني.
٣. إنشاء بنيات تحتية علمية منتشرة في كل الدولة بالشراكة مع القطاع الخاص للتدريب على الأمن السيبراني.
٤. إنشاء مختبرات لتقييم وتحليل مهددات الأمن السيبراني والتحذير منها، وتنمية وتطوير المهارات في المجالات الأساسية للأمن السيبراني.
٥. إنشاء مؤسسات تعليمية لبناء القدرات في مجالات العدالة الجنائية (سلطات انفاذ القانون– الادعاء العام– القضاء).[١٨٩]
٦. تكثيف التأهيل والتدريب في مجال الأدلة الرقمية لمنسوبي الجهات المختصة بالتعامل مع الجريمة الإلكترونية.
٧. إدخال الأمن السيبراني ضمن المساقات الأكاديمية في مؤسسات التعليم العالي وتقديم المنح الدراسية للطلاب لدراسة الماجستير والدكتوراه في الأمن السيبراني.
٨. **تبنى توسيع نطاق دراسة الأمن السيبراني بالجامعات باتخاذ التدابير التالية:**

أ–إنشاء مفوضية خاصة بالتعليم في المجلس الأعلى للأمن السيبراني – المقترح) لتطوير

١٨٨ أنظر استراتيجية استراليا الوطنية لمكافحة الجريمة الإلكترونية، مرجع سابق، ص١٦–١٧:
- Australia National Plan to Combet Cybercrime, Key Priority- Improving the Capacity and Capability of Aqencies to Adress Cybercrime p,16-17 :الموقع الإلكتروني www.ag.gov.av

١٨٩ أنظر السياسة الوطنية الهندية للأمن السيبراني، 2013، مرجع سابق، ص9:
India National Cyber Security Policy. Human Resource Development.p.9

البنيات التحتية للأمن السيبراني.

ب-إضافة دورات عن الأمن السيبراني للمناهج الدراسية في التعليم الجامعي.

ج-توفير الكتب والمجلات والمقالات والوسائل الأخرى باللغة العربية.

د-فتح برنامجين على الأقل- بالجامعات لدراسة الأمن السيبراني اعتبارا من العام الدراسي ٢٠١٥- ٢٠١٦.

هـ-فتح برنامج للدكتوراه لطالب واحد على الأقل في مجال الأمن السيبراني لعام ٢٠١٥-٢٠١٦.

٩. تنفيذ برنامج مباشر للطلاب لاكتساب الخبرات في مجال الأمن السيبراني وذلك بالوسائل التالية:

أ-اعداد برامج دراسية للطلاب الذين يرغبون في التخصص في الأمن السيبراني.

ب-تنظيم معسكرات صيفية للطلاب تركز برامجها على الأمن السيبراني.

ج-تنظيم فعاليات ترويجية لمفهوم الأمن السيبراني في الجامعات.

د-تنظيم مسابقات الدفاع السيبراني Cyber Defence بين الجامعات.[١٩٠]

هـ-تنظيم مسابقات الفيديو أو الملصقات في أمن المعلومات لزيادة الوعى بالأمن السيبراني في مدارس الأساسي والمدارس الثانوية والجامعات.

و-زيادة مقدرات فرق الاستجابة لطوارئ حوادث الحاسب الآلي وتدريب الخبراء ومساعدتهم في اكتساب الخبرة في التنفيذ.

١٠. الترويج لعقد دورات تدريبية في الأمن السيبراني على مستوى مدارس الأساس والمدارس الثانوية وفي مقرات التعليم غير النظامي وذلك من خلال الوسائل التالية:

أ-إضافة الأمن السيبراني لمناهج برامج الحاسب الآلي في المدارس الثانوية المهنية.

ب-إضافة مساق الأمن السيبراني إلى برامج المساقات المقررة لدراسة تقنية المعلومات.

ج-تكثيف نشاطات زيادة مستوى الوعى بالأمن السيبراني لدى مستخدمي الحاسب الآلي وذلك من خلال الندوات والسمنارات ونشاطات التعليم غير النظامي

١٩٠ أنظر استراتيجية اليابان للأمن السيبراني، ١٠ يونيو ٢٠١٣، مرجع سابق، في شأن مفهوم Defence of Cyber-crime، ص٤١.

واستخدام وسائل الإعلام في زيادة الوعى بالأمن السيبراني وبمخاطر الجريمة الإلكترونية.[١٩١]

١. تنمية وتطوير المقدرات البحثية للكوادر المتخصصة في مكافحة الجريمة الإلكترونية بهدف التفوق التقني على المهاجمين بوصفه الوسيلة الوحيدة لكشف اختراقاتهم وجرائمهم ومنعها أو الحد منها.
٢. إنشاء مراكز لأبحاث الأمن السيبراني الدفاعية Cyber DefenceResearchCenters بالتعاون مع قطاع الصناعة كشركاء للقيام بالنشاطات العلمية البحثية بإجراء الدراسات وتحليل مجموعات المهاجمين وطرقهم وخبراتهم في مجالات تقنية المعلومات.
٣. تدوين مفاهيم الدفاع السيبراني كغيرها من الخبرات والنشاطات التدريبية.[١٩٢]
٤. تشجيع استخدام أجهزة حماية الأمن السيبراني التي تلبي على الأقل الحد الأدنى من الحماية المطلوبة وتستخدم بواسطة القطاع العام والخاص.
٥. تسهيل الإبلاغ عن الجريمة الإلكترونية: إن الذين يقعون ضحايا للجريمة الإلكترونية يحتاجون أن يعرفوا أين يتم الإبلاغ والحصول على المساعدة في أقرب وقت ممكن، عدم العلم بذلك يمنع الضحايا من الإبلاغ وبالتالي يحد من قدرة الجهات المختصة من الاستجابة للحادثة والعلم بوقوعها، ولذلك يجب إنشاء آلية لاستلام البلاغات عبر الإنترنت on line تختص بالآتي:

أ- تقديم نصائح تعليمية لمقدم البلاغ.

ب- تحويل البلاغ إلى سلطات إنفاذ القانون والسلطات الأخرى المختصة لمزيد من الاهتمام والتحقيق عندما يكون ذلك مفضلاً.

ج-متابعة تطورات البلاغ وما تم بشأنه.[١٩٣]

---

١٩١ أنظر استراتيجية تركيا الوطنية للأمن السيبراني لعام ٢٠١٣-٢٠١٤، مرجع سابق، ص٣٦-٤١، حيث تم اقتباس مضمون البنود من ٧ إلى ١٠.

Turkey: National Cyber Security Strategy and 2013- 2014 Action Plan, No5-5. Human Resources and Awareness- Raising Activities on Cyber Security,p.38-41.

١٩٢ البنود من (١٠-١٢) أنظر استراتيجية فرنسا لعام ٢٠١١، مرجع سابق، ص١٦.

- France,Strateqy,Information SystemDefence and Scientific.

١٩٣ أنظر استراتيجية استراليا، مرجع سابق، ص١٠-١١.

Australia National Plan to Combet Cybercrime, Educating the Community to Protect - 11-Themselves, p.10

٦. تساعد آلية استلام بلاغات الجريمة الإلكترونية على تحقيق الأهداف التالية:

أ- تقليل الارتباك بشأن كيفية الإبلاغ عن الجريمة الإلكترونية.

ب- تقديم بيانات مجمعة مركزياً عن الجرائم الإلكترونية.

ج- إنسياب تقارير الجريمة الإلكترونية بين سلطات انفاذ القانون والسلطات الأخرى المختصة.

د-تقديم نصائح من جهة مركزية لتفادي الجريمة الإلكترونية.[١٩٤]

المبدأ الرابع: حماية البنيات التحتية الحساسة:

تعد حماية البنيات التحتية الحساسة[١٩٥]لتقنية المعلومات هدف رئيسي للأمن السيبراني، هناك مكونات أساسية لكل البينات التحتية الحساسة وتزداد أهميتها باستمرار، ويجب على السلطات الحكومية المختصة وعلى القطاع الخاص إيجاد وتعزيز قواعد ونظم استراتيجية لتنسيق أكثر تقارباً يعتمد على مشاركة مكثفة في المعلومات ذات الصلة بالأمن السيبراني.

للأسباب المتقدمة يتطلب حماية البنيات التحتية للأمن السيبراني مبادرات جادة من الشركاء في القطاع العام والخاص في مجالات تقنية المعلومات والاتصالات، الشئون المالية، الطيران، السكة حديد، الكهرباء، النفط، الغاز، الحكومة وخدماتها الإدارية وتشمل السلطات العامة المحلية، الخدمات الطبية، المياه والامدادات، على أن تكون تدابير الحماية وفقاً لما أقرته المؤسسات الحكومية وغير من الجهات المعتمدة، ومن الضروري تقوية معايير وتدابير الحماية كلما كان ذلك مناسبا.[١٩٦]

لتحقيق أهداف حماية البينات التحتية الحساسة من الاختراقات والهجمات الإلكترونية تتبع التدابير التالية:

١. الحد من الاختراقات وإتلاف الشبكات بالوسائل التقنية المتطورة.

---

١٩٤ لبنود من ١٠ إلى ١٢ أنظر استراتيجية فرنسا لعام ٢٠١١، مرجع سابق، ص١٦.
France›s Strategy, Information System Defense and Security, Enhance and Perpetuate our Scientific, technical, Industrial and Human Capabilities, p.16.

١٩٥ تعرَّف البينات التحتية الحساسة بأنها ''أساسيات حياة الناس الاجتماعية ونشاطاتهم الاقتصادية، التي تقدم خدمات مختلفة لا يمكن تعويضها بأي طريقه أخرى كخدمات المياه والكهرباء والصرف الصحي والطرق والسكة حديد والطيران والتعليم والصحة ومحطات التلفزيون والإذاعة وأنظمة تقنيات المعلومات والشبكات... الخ، وغالبية هذه الخدمات يعتمد على أنظمة وبرامج الحاسب الآلي والهجوم الإلكتروني على أنظمة تشغيلها بسبب إضرار قد تؤدى تعطيل الخدمات أو إيقافها مؤقتاً أو حتى تدمير البنيات التحتية التي تقدم هذه الخدمات مما يؤثر على حياة الناس ونشاطاتهم، لمزيد من التفاصيل، أنظر استراتيجية اليابان للأمن السيبراني، ١٠ يونيو ٢٠١٣، مرجع سابق، ص٢٤، هامش٥٩.

١٩٦ أنظر استراتيجية اليابان للأمن السيبراني، ١٠ يونيو ٢٠١٣، مرجع سابق، ص٢٤، تحت العنوان: Roles of Critical infrastructure Providers.

٢. التأكيد على فعالية إدارة حوادث الأمن السيبراني وعلى صمود البنيات التحتية لتقنية المعلومات وعلى استعادتها مقدراتهافي أسرع وقت ممكن بعد الهجوم الإلكتروني عليها.

٣. حماية صمود البنيات التحتية يتطلب الآتي:

أ- إعداد خطط لحماية البنيات التحتية لتقنية المعلومات بالتعاون مع القطاع الخاص، وأن تشمل الخطط إنشاء آليات لتأمين المعلومات أثناء عمليات إرسالها أو استخدامها أو تخزينها وإيجاد دليل ومعايير.

ب- إعداد خطة أو خطط لإدارة الأزمات.

ج- تفعيل التقييم الأمني لأوضاع البنيات التحتية لأنظمة تقنية المعلومات.

د- تشغيل مراكز وطنية لحماية البنيات التحتية الحساسة لتقنية المعلومات على مدار ٢٤ ساعة يومياً، على أن تشكل هذه المراكز نموذجاً لحماية البنيات التحتية الحساسة لتقنية المعلومات في الدولة.

هـ- تسهيل العمليات التالية:

- التعرف المخاطر والمهددات.
- التقييم الأمن السيبراني للبنيات التحتية الحساسة.
- معالجة الخلل والثغرات والحماية.
- توفير الموارد الأساسية التي تعتمد عليها خطة حماية البنيات التحتية.

و- إعداد جدول (مصفوفة) لتنفيذ أفضل التجارب والخبرات العالمية لحماية البنيات التحتية الحساسة لتقنية المعلومات Critical Information Infrastructure للحد من مخاطر الهجمات الإلكترونية وتحسين الوضع الأمني.

ز- تشجيع وتحديد استخدام منتجات تقنية بعينها تتوفر فيها المعايير المطلوبة للأمن السيبراني.

ح- إجراء فحص أمني دوري للبنيات التحتية الحساسة لتقنية المعلومات.[١٩٧]

---

١٩٧ أنظر سياسة الهند الوطنية للأمن السيبراني، ٢٠١٣، مرجع سابق، ص٧-٨ تحت العنوان التالي:
India National Cyber Security Policy (2013),op.cit.

٤. برنامج إدارة أمن المعلومات في البينات التحتية الحساسة: يتطلب البرنامج الإجراء الآتي:

أ- تحديد البنيات التحتية الحساسة التي من المحتمل أن تكون أهدافاً مباشرة للتهديدات والتي قد تؤدي إلى الإخلال بالنظام العام في حالة التعطيل أو التدمير.

ب- تحديد جهات قطاعية مختصة للقيام بعمليات تحليل المخاطر في البينات التحتية المهددة.

ج- تحديد الطرق التي تتبعها الجهات القطاعية المختصة في التحليل.

د- تحديد متطلبات خطط الطوارئ القطاعية.

هـ- تقديم تقارير دورية وسنوية عن تحليل المخاطر.

و- تحديد متطلبات تنفيذ استمرارية خطط قطاعات الأعمال.

ز- تحديد وتنفيذ الاحتياطات الأمنية القطاعية.

ح- تجهيز وثيقة تتضمن الحد الأدنى للمتطلبات الأمنية التي يجب إتباعها في المؤسسات العامة.

ك- دورات تدريبية في الأمن السيبراني لمديري أنظمة تقنية المعلومات والكوادر الفنية الأخرى ذات الصلة مع مراعاة أولويات الاحتياجات التدريبية والإقرار بمهنية الذين تم تدريبهم.

ل- نشر وتحديث المطبوعات والمعايير الخاصة بأمن تقنية المعلومات.[١٩٨]

٥. تقوية البنيات التحتية للتدريب في مجال الأمن السيبراني، يتم ذلك بالوسائل التالية:

أ- دورات قصيرة للمدراء الكبار top managers المسؤولين عن أنظمة المعلومات والأمن السيبراني في المؤسسات العامة.

ب- تدريب الكوادر الفنية ومنحهم الشهادات التي توضح نوع ومستوى التدريب.

ج- توفير التدريبات للمدققين الذين يعملون بالمؤسسات العامة لمساعدتهم على رفع الكفاءة للقيام بفحص معايير الأمن السيبراني في أنظمة المعلومات.[١٩٩]

٦. إقرار القواعد والإجراءات التي تساعد على حماية أمن تداول البيانات بين المؤسسات العامة.

---

١٩٨ أنظر استراتيجية تركيا الوطنية للأمن السيبراني وخطة العمل، ٢٠١٣- ٢٠١٤، مرجع سابق، ص٢٨-٢٩ تحت العنوان التالي:
.Turkey: National Cyber Security Strategy and 2013- 2014 Action Plan

١٩٩ استراتيجية تركيا، المرجع السابق، ص٣٠، تحت العنوان التالي:
Strengthening the National Cyber Security Infrastructure.No7.p-30

٧. إعداد وتنفيذ برنامج أمن البرمجيات Software Security program
٨. إعداد وتنفيذ مشروع لمنع التهديدات السيبرانيةCyber Threats Prevention Project.
٩. إصدار الشهادات بتوفر معايير الجودة للمنتجات والخدمات في مجال الأمن السيبراني.
١٠. إقرار القواعد التي يتم بموجبها منح الشهادات لمقدمي خدمات الحاسب الآلي الفنية[٢٠٠]

المبدأ الخامس: التعاون الدولي:

الجريمة الإلكترونية مشكلة عالمية تستهدف مؤسسات القطاع العام والخاص والأفراد وقد يكون الاستهداف من داخل الدولة أو من خارجها من أي مكان في العالم، والحكومات الوطنية لا تستطيع مواجهة هذه المشكلة وحلها بمفردها، وفي حين أن الحكومات تستطيع القيام بالتنظيم التشريعي داخل حدود أوطانها إلا أنها لا تستطيع ذلك خارج حدودها، وهناك ما يدعو للتأكيد على أن الدول قادرة على دعم الحرب ضد الجريمة الإلكترونية، وفقاً للمعايير الدولية.

ويمكن تسهيل التعاون الدولي في مواجهة الجريمة الإلكترونية عندما تتضمن النظم التشريعية المختلفة للدول النص على جرائم مشتركة تسمح لسلطات التحقيق والادعاء العام بمباشرة إجراءاتها بشأن الجريمة المرتكبة بغض النظر عن الاختصاص المكاني الذي ارتكبت فيه الجريمة أو مهما كان المكان الذي وجدت فيه أدلة الجريمة، وتسمح الجرائم المشتركة common offences – في النظم التشريعية المختلفة – بإمكانية تسليم المجرمين وفقاً لشروط اتفاقيات تسليم المجرمين.

لتحقيق أهداف التعاون الدولي يجب اتخاذ التدابير التالية:

١. إنشاء شبكة واسعة من الشركاء الخارجيين من أجل تبادل البيانات الأساسية، مثال ذلك، نقاط الضعف أو عيوب المنتجات والخدمات.
٢. في الفضاء السيبراني، تستخدم الدول والأقاليم ذات الحماية المتدنية للأمن السيبراني Vulnerable countries كمنصات لإطلاق الهجمات الإلكترونية، وتختلف المقدرات التقنية للدول في الاستجابة للهجمات الإلكترونية ومواجهتها، وهذا الموقف يقود لتكوين رأي عام في المجتمع الدولي بضرورة التعاون للتصدي للهجمات الإلكترونية لأن أثرها الضار والمدمر قد لا يكون محدوداً.
٣. تقديم الدعم للدول التي تنطلق منها الهجمات الإلكترونية لتطوير مقدراتها وقدرات الفنيين المختصين للتعامل مع هجمات الجريمة الإلكترونية.

٢٠٠ استراتيجية تركيا، المرجع السابق، ص ٣٢-٣٤، البنود ٩ إلى ١٣.

٤. إنشاء مراكز (CERTs) الوطنية لتفعيل التعاون الدولي وتقديم الدعم للدول الأخرى التي لا تسمح إمكاناتها بانشاء مراكز (CERT).[٢٠١]
٥. التوقيع والتصديق على الاتفاقيات الإلكترونية والأمن السيبراني التي تخدم المصلحة العامة لكافة دول العام.
٦. عقد الندوات والمؤتمرات المحلية والإقليمية والدولية في مجالات الجريمة الإلكترونية.
٧. الانضمام للتحالفات الإقليمية والدولية في مواجهة الجريمة الإلكترونية كلما كان ذلك يحقق المصلحة العامة في هذا المجال.

٢٠١ أنظر استراتيجية اليابان للأمن السيبراني، ١٠ يونيو ٢٠١٣، مرجع سابق، تحت العنوان: Global Outreach,p.50-52

المراجع

References

أولاً: الاستراتيجيات:Strategies

١- مشروع الاستراتيجية العربية لمواجهة الجرائم الإلكترونية، الذي أصدرتهاالأمانة العامة لمجلس وزراء الداخلية العرب عام ٢٠١١.

٢- استراتيجيات الدول الأجنبية لمواجهة الجريمة الاليكترونية (مراجع أساسية) :

1- Australia: Cyber Security Strategy (2011) .

2- Canada: Cyber Security Strategy (2010) .

3- France: Information System Defense and Security Strategy (2011) .

4- Germany: Cyber Security Strategy (2013) .

5- Japan: Information Security Strategy for Protecting Nation (2013).

6- India: National Cyber Security Policy (2013).

7- Switzerland: National Strategy for Protection Switzerland against Cyber risks, (2012)

8- Turkey: National Cyber Security Strategy and 2013- 2014 Action Plan.

9- United Kingdom: Cyber Crime Strategy (2010).

10- United Kingdom: Cyber Security Strategy (Nov. 2011) .

11- USA: International Strategy For Cyberspace Prosperity, Security and Openness in a Networked World (May 2011).

ثانياً: التقارير: Reports

- The UK Cyber Security Strategy Report on Progress and Forward Plans – (Dec. 2014).
- Report of The Chairman of High Level Experts Group (HLEG), Global Cyber Security Agenda, International Technology Union (ITU), 2007.

ثالثاً: الدراسات: Studies

- National Cyber Security Strategies in the World, European Agency for Network and Information Security, Feb. 2013 , Brussels .

- Net Losses: Estimating the Global Cost of Cybercrime, Economic Impact of Cybercrime II Center for Strategic and International Studies, June 2014.
- Alexander Seger, Cybercrime Strategies, Discussion paper, Global Project on Cybercrime, Council of Europe, Strasbourg, France, 30 Mar 2012.

ملحق رقم (٢)

استعراض تاريخي مختصر لمراحل الجريمة الاليكترونية وتطوراتها

من أ-ك

WAVEFRONT
CONSULTING GROUP
CERTIFIED INFORMATION
SECURITY CONSULTANT

A BRIEF HISTORY OF CYBERCRIME

These pages list the major events in the use of computers and computer networks to commit criminal acts, starting in the 1970's to the present day. This list was put together as part of our course Introduction to Computer Crime Studies (FSCT7220) presented at BCIT. The list is not meant to be comprehensive, but it is meant to be representative. If you notice any errors or serious omissions, please contact us.

Section 1 - 1970-1990

1971

- John Draper discovers the give-away whistle in Cap'n Crunch cereal boxes reproduces a 2600Hz tone. Draper builds a 'blue box' that, when used with the whistle and sounded into a phone receiver, allows phreaks to make free calls. Esquire publishes "Secrets of the Little Blue Box" with instructions for making one. Wire fraud in the US escalates.

- A rogue program called the Creeper spreads through early Bulletin Board networks

1972

- The Inter Networking Working Group is founded to govern the standards of the Internet. Vinton Cerf is the chairman and is known as a "Father of the Internet".

1973

- Teller at New York's Dime Savings Bank uses a computer to embezzle over $2 million

1978

- First electronic bulletin board system (BBS) appears; becomes the primary means of communication for the electronic underground..

1981

- Ian Murphy, aka. "Captain Zap", becomes first felon convicted of a computer crime. Murphy broke into AT&T's computers and changed the billing clock so that people receive discounted rates during normal business hours.

1982

- Elk Cloner, an AppleII boot virus, is written.

1983

- Movie WarGames introduces public to the phenomenon of hacking (actually war-dialing).
- US Secret Service gets jurisdiction over credit card and computer fraud.

1984

- Phiber Optik forms Masters of Deception hacking group.
- US Comprehensive Crime Control Act gives Secret Service jurisdiction over computer fraud.
- Hacker magazine 2600 begins publication (still in print; see Captain Crunch for the derivation of the name).

1985

- Online hacking magazine Phrack established.

1986:

- Pakistani Brain, the oldest virus created under unauthorized circumstances, infects IBM computers.
- After many break-ins into govt. and corporate computers, Congress passes the Computer Fraud and Abuse Act, making this a crime. The law does not cover juveniles.

1987

- Computer Emergency Response Team (CERT) created.

1988

- Kevin Mitnick secretly monitors the e-mail of MCI and DEC security officials. He is convicted and sentenced to a year in jail.
- Kevin Poulsen is indicted on phone-tampering charges. He goes on the run and avoids capture for 17 months.
- First National Bank of Chicago is the victim of $70-million computer theft.
- Robert T. Morris, Jr., graduate student at Cornell University and son of a chief scientist at the NSA, launches a self-replicating worm (the Morris Worm) on the government's ARPAnet (precursor to the Internet). The worm gets out of hand and spreads to over 6000 networked computers,

clogging government and university systems. Morris is dismissed from Cornell, sentenced to three years' probation, and fined $10K.

1989

- First large-scale computer extortion case is investigated - under the pretence of a quiz on the AIDS virus, users unwittingly download a program which threatens to destroy all their computer data unless they pay $500 into a foreign account.

- Hackers in West Germany (loosely affiliated with the Chaos Computer Club) are arrested for breaking into US government and corporate computers and selling operating-system source code to the KGB.

1990

- The Electronic Frontier Foundation (EFF) is formed.

- Legion of Doom and Masters of Deception engaged in online warfare - jamming phone lines, monitoring calls, trespassing in each other's private computers.

- After a prolonged sting investigation, Secret Service agents swoop down on organizers and members of BBS's in 14 US cities, including the Legion of Doom. The arrests are aimed at cracking down on credit-card theft and telephone and wire fraud.

1991

- Kevin Poulsen is captured and indicted for selling military secrets.

1992

- Dark Avenger releases 1st polymorphic virus.

1993

- During radio station call-in contests, hacker-fugitive Kevin Poulsen and friends rig the stations' phone systems to let only their calls through. They win two Porsches, vacation trips and $20,000.

- First DefCon hacker conference held in Vegas.

1994

- 16-year-old student, nicknamed "Data Stream", arrested by UK police for penetrating computers at the Korean Atomic Research Institute, NASA and several US govt. agencies.

- Five members of the Aum Shinri Kyo cult's Ministry of Intelligence break into Mitsubishi Heavy Industry's mainframe and steal Megabytes of sensitive data.

- Hackers adapt to emergence of the World Wide Web, moving all their how-to information and hacking programs from the old BBS's to new hacker Web sites.

1995

- Russian crackers steal $10 million from Citibank. Vladimir Levin, the ringleader, uses his work laptop after hours to transfer the funds to accounts in Finland and Israel. He is tried in the US and sentenced to 3 years in prison. All but $400K of the money is recovered.

- The French Defence Ministry admits Hackers succeeded in stealing acoustic codes for aircraft carriers and submarines

- Movies 'The Net' and 'Hackers' released.

- Hackers deface federal web sites.

- Macro viruses appear.

- Kevin Mitnik arrested again for stealing credit card numbers. He is jailed on charges of wire fraud and illegal possession of computer files stolen from Motorola and SUN. He remains in jail for 4 years without trial.

1996

- John Deutsh, CIA director, testifies foreign organized crime groups behind hacker attacks against the US private sector.

- US Communications Decency Act (CDA) passed – makes it illegal to transmit indecent/obscene material over Internet.

- Canadian hackers (the 'Brotherhood') break into CBC.

- South Korean media reports that North Korean government officials are engaging in efforts to obtain foreign proprietary technology through indirect methods .Bell Research Labs in the US announce they have found a way to counterfeit the electronic money on smart cards.

- The US General Accounting Office reports hackers attempted to break into Defense Dept. computer files 250,000 times in 1995. About 65% of these attempts were successful.

1997

- Freeware tool AOHell is released - allows unskilled hackers (script kiddies) to wreak havoc on America Online.

- US Supreme court strikes down Communications Decency Act (CDA).

- America On-line (AOL), one of the largest Internet service providers in the US, cuts direct access for its users in Russia due to the high level of fraud.

- The German Chaos Computer Club claims it was able to penetrate Microsoft's Internet software and the financial management program Quicken, and transfer money between accounts without either the account holder or bank realizing the transaction was unauthorized.

- FBI's National Computer Crimes Squad reports 85% of companies have been hacked, and most never know it.

1998

- Hacking group Cult of the Dead Cow releases a Trojan horse program called Back Orifice at Defcon. Once installed a Windows 9x machine the program allows for unauthorized remote access.

- Timothy Lloyd is indicted for planting a logic bomb on the network of Omega Engineering, causing millions in damage.

- Hackers alter The New York Times Web site, renaming it HFG (Hacking for Girlies).

- During heightened tensions in the Persian Gulf, hackers break-in to unclassified Pentagon computers and steal software programs.

- Information Security publishes its first annual Industry Survey, finding that nearly three-quarters of organizations suffered a security incident the prior year.

- L0pht testifies to the senate that it could shut down nationwide access to the Internet in less than 30 mins.

1999

- The Melissa worm is released and becomes the most costly malware outbreak to date (Mar).

- US Defense Dept. acknowledges 60-80 attacks per day (Mar)

- Kevin Mitnick, detained since 1995 on charges of computer fraud, signs plea agreement (Mar).

- The April 26 CIH virus strikes individual PC users around the world. Less common than Melissa, CIH was intended to overwrite hard drives, erasing everything on them (Apr)

- The US Justice Dept. declines to prosecute former CIA Director John

Deutch for keeping 31 secret files on his home computer after he left office in 1996 (Apr)

- David Smith pleads guilty to creating and releasing the Melissa virus. It's one of the first times a person is prosecuted for writing a virus (Dec).

2000:

- Russian cracker attempts to extort $100K from online music retailer CD Universe, threatening to expose thousands of customers' credit card numbers. He posts them on a website after the attempted extortion fails.
- Barry Schlossberg (aka. Lou Cipher) is successful at extorting 1.4M from CD Universe for services rendered in attempting to catch the Russian hacker. (Jan)
- Denial of Service (DoS) attacks by 'Mafia Boy' on eBay, Yahoo! and other popular sites render them temporarily unavailable to their users (and cause those companies significant financial losses) (Feb)
- Activists in Pakistan and the Middle East deface Web sites belonging to the Indian and Israeli govts. to protest oppression in Kashmir and Palestine.
- Hackers break into Microsoft's corporate network and access source code for the latest versions of Windows and Office software.
- A news release issued by Internet Wire, and reported by Bloomberg and other news organizations, causes Emulex stock to plunge from $110 a share to $43 on the NASDAQ exchange in minutes. A former Internet Wire employee, believed to have authored the bogus story, faced charges and is alleged to have pocketed $241,000 short-selling Emulex shares that day (Aug).
- Distributed Denial of Service (DDoS) attacks are launched against : Yahoo, eBay, CNN.com, Amazon.com, Buy.com, ZDNet, E*Trade, etc.
- Pres. Clinton says he doesn't use e-mail to communicate with his daughter Chelsea at college, because he doesn't think the medium is secure.
- The "I Love You" virus spreads quickly by causing copies of itself to be sent to all individuals on the affected computer's address book (by attaching VBScript executable code to e-mails) (May).
- SANS releases its first "Top 10 Vulnerabilities" list, denoting the most prevalent problems exploited by hackers.
- Kevin Mitnik is released from prison (Jul).
- FBI establishes fake security start-up company in Seattle and lures two

Russian citizens to U.S. soil on the pretense of offering them jobs, then arrests them. The Russians are accused of stealing credit card information, attempting to extort money from victims, and defrauding PayPal by using stolen credit cards to generate cash. (Nov).

2001

- Microsoft falls victim of a new type of attack against domain name servers, corrupting the DNS paths taking users to Microsoft's Web sites. This is a Denial of Service (DoS) attack. The hack is detected within hours, but prevents millions of users from reaching Microsoft Web pages for two days.
- The L10n worm is discovered in the wild attacking older versions of BIND DNS.
- Dutch cracker releases Anna Kournikova virus, initiating wave of viruses tempting users to open infected attachments by promising a sexy picture of the Russian tennis star (Feb).
- FBI agent Robert Hanssen is charged with using his computer skills and FBI access to spy for Russia (Mar).
- Code Red, the first polymorphic worm, infects tens of thousands of machines (Aug).
- Spurred by rising tensions in Chinese-American relations, US and Chinese hackers engage Web defacement skirmishes. (May)
- Antivirus experts identify Sadmind, a new cross-platform worm that uses compromised Sun Solaris boxes to attack Windows NT servers. (May)
- Russian programmer Dmitry Sklyarov is arrested at the annual Defcon hacker convention. He is the first person criminally charged with violating the Digital Millennium Copyright Act (DMCA). (Jul)
- The Nimda memory-only worm wreaks havoc on the Internet, eclipsing Code Red's infection rate and recovery costs. (Sept)
- Napster shuts down after legal challenges from the recording industry and Metallica.
- The 9/11 World Trade Center and Pentagon terrorist attacks spark lawmakers to pass a barrage of anti terrorism laws (incl. the Patriot Act), many of which group Hackers with terrorists, and remove many long standing personal freedoms in the name of safety.
- Microsoft and its allies vow to end "full disclosure" of security vulnerabilities by replacing it with "responsible" disclosure guidelines.

- EU publishes report on its investigation of the ECHELON system, purportedly used by the US, UK, Canada, Australia and NZ to spy on radio, telephone and Internet communications. Meant for military and defense use, there is suspicion it is being used to invade personal privacy and for commercial spying.

- EU adopts a controversial cybercrime treaty which makes the possession and use of hacking tools illegal (Nov)

2002

- Bill Gates decrees that Microsoft will secure its products and services, and kicks off a massive internal training and quality control campaign (trustworthy computing) (Jan)

- An Information Security survey finds that most security practitioners favor full disclosure since it helps them defend against hacker exploits and puts pressure of software vendors to improve their products.

- Roger Duronio, UBS PaineWebber sys-admin, plants a logic bomb which costs $3M+ in losses/repairs (Mar)

- The Klez.H worm becomes the biggest malware outbreak in terms of machines infected, but causes little monetary damage (May).

- Shadowcrew's Web site appears, with forums for information on trafficking in personal information (Aug)

2003

- SQL Slammer, targeting MS SQL Server, becomes fastest spreading worm in history (Jan).

- U.S. convicts Kazakhstan cracker of breaking into Bloomberg L.P.'s computers and attempting extortion (Feb).

- Former employee of Viewsonic arrested, charged with hacking into company's computer and destroying data. (Feb)

- MS Blaster worm and variants (Welchia) released, arrests follow (Aug).

- A worm disables critical safety systems at a nuclear power plant in Ohio (Aug).

- RIAA (Recording Industry Association of America) sues 261 people for distributing MP3s over P2P networks (Sep).

- U.S. Justice Department announces more than 70 indictments and 125

convictions or arrests for phishing, hacking, spamming and other Internet fraud as part of Operation CyberSweep. (Nov)

- Microsoft offers $250K each for information leading to the arrest and conviction of those responsible for unleashing the MSBlast.A worm and Sobig virus (Nov)
- Two men hack into wireless network at Lowe's store in Michigan and steal credit card information (Nov).

2004

- Brian Salcedo sentenced to 9 years for hacking into Lowe's home improvement stores and attempting to steal customer credit card information. Prosecutors said three men tapped into the wireless network of a Lowe's store and used that connection to enter the chain's central computer system in NC, installing a program to capture credit card information.
- Multiple variants of MyDoom worm released to launch DoS attacks against SCO and Microsoft. Netsky, Sasser, Bagel, Sober follow (Feb).
- Secret Service seizes control of the Shadowcrew Web site and arrests 28 people in 8 states and 6 countries. They are charged with conspiracy to defraud the US. Nicolas Jacobsen, is charged with hacking into a T-Mobile computer system, exposing documents the Secret Service had e-mailed to an agent. (Operation Firewall, Oct)
- CERT stops tracking number of security incidents.
- US CAN-SPAM act passed to prosecute spammers. Jeremy Jaynes & Jessica DeGroot first to be convicted under CAN-SPAM act (Jaynes sentenced to 9 years). (Nov)

2005

- Netcraft survey estimates more than 60M web sites online.
- Paris Hilton's T-Mobile phone is hacked, and photos and celebrity private phone numbers posted on Web (Feb).
- Choicepoint acknowledges that thieves posing as legitimate businessmen accessed 145K consumer records, including credit reports and Social Security Numbers. (Feb)
- Bank of America has 1.2M names and Social Security numbers stolen (Feb).
- Juju Jiang sentenced to 27 months for installing keyloggers at Kinkos locations in NY; used confidential information to access individual bank accounts (Feb)

- FBI's e-mail system is hacked (Feb)
- Lexis Nexis announces hackers have stolen private information on 32K people, including Social Service Numbers (SSN's) and passwords (Mar)
- Undisclosed application security issue on Cisco's site forces global password reset (Mar)
- DSW/Retail Ventures – 100,000 accounts hacked; Boston College – 120,000 accounts hacked (Mar)
- BJ's Wholesale Club – information on 40K credit cards stolen from outsourcer IBM (Mar).
- Keystroke loggers are used in heist at Sumitomo Mitsui Bank in London almost nets thieves £220M (Mar)
- Lexis-Nexis – another 280,000 account passwords compromised (Apr).
- Polo Ralph Lauren/HSBC – 108,000 accounts hacked; DSW/Retail Ventures – 1.3M more accounts hacked (Apr)
- Wachovia/Bank of America/PNC Financial Group/ Commerce Bancorp – insiders hack 670K+ accounts (Hackensack) (Apr)
- The Samy worm at MySpace makes everybody Samy's friend (Apr)
- Tel Aviv Magistrate's Court remanded several people from some of Israel's leading commercial companies and private investigators suspected of commissioning and carrying out industrial espionage against their competitors, which was carried out by planting Trojan horse software in their competitors' computers. (Apr)
- CardSystems admits hackers planted virus and accessed 14M credit card numbers (potentially 40M); company folds (Jun)
- Boston College - 120K accounts hacked (Mar); Tufts University – 106K accounts hacked (Mar); University of Hawaii – insider compromises 150K accounts (Jun); University of Connecticut – 72K accounts hacked (Jun); University of Southern California – 270K accounts hacked (Jul); University of Utah – 100K accounts hacked (Aug).
- Allan Carlson convicted of computer and identity fraud, sentenced to 48 months; spoofed e-mails complaining about poor performance of Philadelphia Phillies (Jul)

- Canada's 'Prince of Pot', Marc Emery, is arrested on a US indictment charging him with selling millions of dollars worth of marijuana seeds over the Internet to customers throughout the US (Jul)

- US Air Force – 33,300 accounts hacked (Aug)

- Zotob worm attacks Windows 2000 computers (Aug)

- Microsoft wins $7M settlement against Spam king Scott Richter, plus promise to stop future spamming (Aug)

- Insufficient authorization on Verizon's MyAccount feature allows users to view each other's information (Aug).

- 3,800 customer credit-card numbers stolen in attack on Guidance Software web site (Nov)

- Janus Mutual Fund uses predictable identifier to authenticate its share holders, enabling them to vote for others (Dec).

- Breaches at Sam's Club, OfficeMax and an unnamed ATM network result in an increase of debit card fraud.

- Chinese cyber-espionage ring code-named 'Titan Rain' hacks into US military bases, defense contractors and aerospace companies.

- Equifax and TransUnion, Canada's main credit bureaux, receive an average of 1,600 calls / month regarding the theft of financial or credit information.

- Information warehousing companies (Choicepoint, Lexis Nexis, CardSystems, Equifax, TransUnion) are popular targets since they possess volumes of information on private individuals.

- PhoneBusters reports 11K+ Identity Theft complaints in Canada, and total losses of $8.5M, making this the fastest growing form of consumer fraud in North America.

2006

- Hackers break into Department of Homeland Security computers, install malware, and transfer files to a remote Chinese-language Web site; Unisys (the contractor) charged with covering up the intrusion.

- HP Chair Patricia Dunn uses pretexting to obtain home phone records of board of directors. (Sep)

- Bulk e-mailer Scott Levine of Snipermail.com gets 8 year prison sentence

for stealing more than 1B personal records from Acxiom, a data repository company (back in '05).

- Private information of Canadian gun owners exposed on Canadian Federal Gun Registry (Mar).
- Stolen Boeing laptop exposes personal information on 3.6K employees (Apr).
- Ohio University alumni relations server compromised and 137K SSN's stolen (April); separate hacks in May lead to further thefts.
- Westjet settles with Air Canada for $15.5M, concluding a lawsuit Air Canada filed in 2004 accusing its rival of illegally accessing confidential data from an employee website (May).
- US Dept. of Veterans' Affairs information stolen from employee's home (28M identities stored on laptop) (May); an additional 2.1M added to list in June; laptop recovered in June; FBI claims no data stolen.
- Personal information of Humana Medicare customers compromised when insurance company employee called up the data through a hotel computer and then failed to delete the file (17K) (June) .
- Hackers access credit card and other personal information of customers who purchased DSL equipment from AT&T's online store (20K) (Aug).
- Hacker accesses Linden Lab's Second Life database and steals unencrypted account names, real life names and contact information, and encrypted passwords and payment data. Second Life is a 3-D virtual world. (Sept).
- Hackers seize control of 78 BC government computers for two months before being detected. They loade porn movies on to the computers, using the government's network as part of a pay-for-porn business. (Feb)
- Fedex exposes 8.5K W2 employee tax forms (Feb).
- A bank machine in Virginia Beach is reprogrammed to dispense $20 bills in place of $5 bills. The machine was left this way for 9 days before someone mentioned the discrepancy to the store clerk. (Aug)
- Alabama nuclear power plant shut down due to excessive network traffic (Aug)
- According to a Gartner study, the 1.5M Americans were victims of Identity Theft in 2006 victim. Every minute 28½ people become victims, or a new victim approx. every 2 seconds.

2007

- Retailer TJMaxx (Winners, Homesense) notifies consumers that server breaches between July 2005 and January 2007 had exposed personal data (45M+ debit and credit cards, $180M direct cost so far) (Jan).
- Payment services firm MoneyGram notifies consumers that server breaches exposed personal data (80K) (Jan).
- Nokia Canada Web Site defaced using an XSS attack (Jan).
- A priority code used to get a free platinum pass to MacWorld was validated on the client, enabling anyone get free passes (Jan) (A similar hack works in 2008).
- Online payment services firm E-Gold charged with money-laundering (Apr) (convicted in 2008)
- AG's from several US States demand that NewsCorp's social networking site MySpace provide list of sex offenders who have registered at the site (May).
- The Chinese government and military are accused of hacking other nations' networks, including US pentagon networks, and German and UK government computers.
- DoS attacks are launched against various government websites in Estonia, including the country's police, Min. of Finance and parliament (May).
- Oracle files lawsuit against SAP, charging that the company's TomorrowNow subsidiary had inappropriately downloaded software patches and documents from Oracle's online support service (Mar).
- Monster.com and other job sites are hacked and resume information stolen (Aug).
- Hackers post sensitive information on 1.2K e-Bay users to forum for preventing fraud on the auction site (Sep)
- TD Ameritrade announces that a compromised company computer had leaked the e-mail addresses of all its 6.3M customers from July 2006 (used for pump and dump spam). E*Trade suffers from similar attack (Sep).
- US Secret Service arrest security consultant Max Ray Butler ('Max Vision') for managing an identity theft ring on the online credit-counterfeiting forum, CardersMarket (Sep)
- A known vulnerability in the helpdesk software used by hosting provider Layered Technologies results in information leakage, including names, addresses, phone numbers and email addresses of up to 6,000 of the company's clients (Sep).

- A hacker exploits a leftover admin function on eBay to block users and close sales (Oct).

- The Storm Worm (a bot program first spotted in Jan), continues to spread spam, promote pump&dump schemes; hides bot computers with DNS fluxing, launches DoS attacks against machines probing its bots.

- Russian Business Network (RBN) offers bulletproof hosting, allowing sites which host illegal content to stay online despite legal takedown attempts. Sept's attack on Bank of India, various MPack attacks use RBN services. (Oct)

- A flaw in Passport Canada's website allows access to the personal information - social insurance numbers, dates of birth and driver's licence numbers - of other people applying for new passports (Nov).

- Infamous Russian malware gang RBN use SQL injection to penetrate US government sites (Nov).

- A vulnerability in WordPress allows spammers to penetrate Al Gore's web site, modify pages, and post spam comments (Nov)

- John Schiefer (LA) admits to using botnets to illegally install software on at least 250K machines and steal the online banking identities of Windows users. (Dec)

2008

- FTC settles with "Life is Good" (www.lifeisgood.com), which exposed credit card information due to SQL Injection flaw (Jan)

- Login page of Italian bank (Banca Fideuram) replaced using XSS (Jan)

- RIAA website DoS'ed, then defaced, using SQL Injection&XSS (Jan)

- CSRF used to hack a Korean e-commerce site (Auction.co.kr) and steal information on 18M users (Feb)

- MySpace and FaceBook private pictures exposed on-line using URL manipulation (Jan & Mar)

- Hackers steal 4.2M card numbers of Hannaford shoppers, resulting in over 2000 fraud cases (Mar)

- SQL and iFrame Injection are used to add Javascript code to websites which then download viruses and other malware from hacker sites when browsed. Search Engine Optimization (SEO) techniques result in infected

pages being placed high on Googles' search results. Affected sites number in excess of 200K. (Mar)

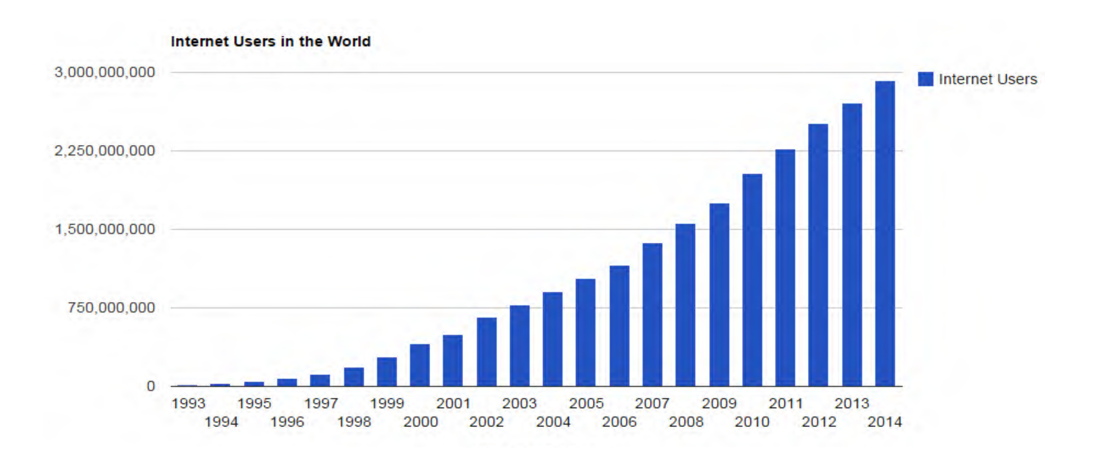
- Just before the Pennsylvania Democratic Primary, XSS is used to redirect users of Barack Obama's website to Hillary Clinton's (Apr)
- US Federal prosecutors charge parent who allegedly badgered a girl to suicide on MySpace with three counts of computer crime (conspiracy and hacking) (May)
- Radio Free Europe hit by DDoS attack (May)
- Online payment service E-Gold pleads guilty to money laundering (Jul)
- Canadian Teachers Federation proposes adding Cyber-Bullying to Canadian Criminal Code (Jul)
- Canadian porn site SlickCash pays $500K to Facebook after it tried to gain unauthorized access to Facebook's friend-finder functionality back in June 2007 (Jul)
- Terry Childs, San Francisco City network admin, refuses to give out passwords, locking other admins out of network (Jul).

ملحق رقم (٣)

مستخدمي الإنترنت حول العالم

من أ-ط

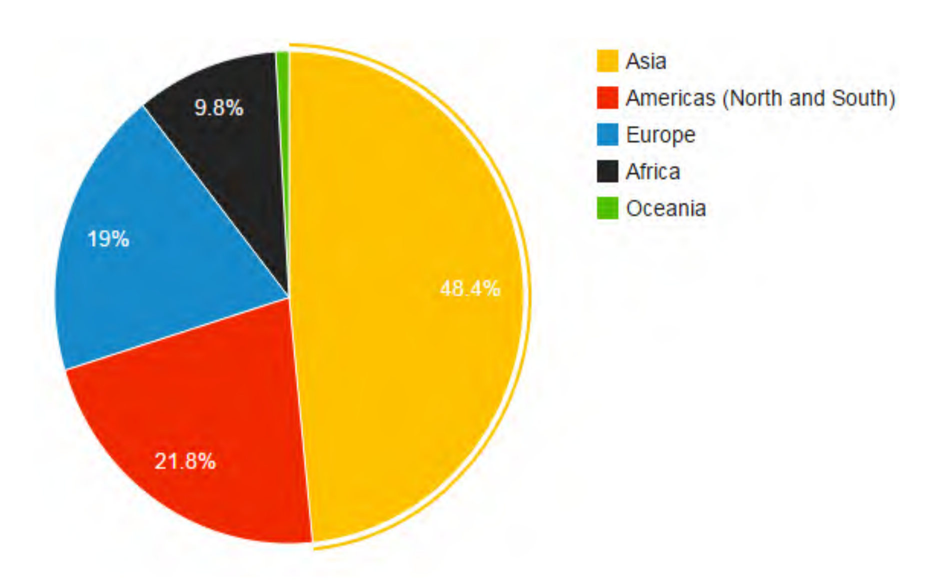
INTERNET USERS 3,046,847,078
INTERNET USERS IN THE WORLD



Around 40% of the world population has an internet connection today (view all on a page). In 1995, it was less than 1%. The number of internet users has increased tenfold from 1999 to 2013. The first billion was reached in 2005. The second billion in 2010. The third billion in 2014. The chart and table below show the number of global internet users per year since 1993:

Year (July 1)	Internet Users	Users Growth	World Population	Population Growth	Penetration (% of Pop. with Internet)
2014*	2,925,249,355	7.9%	7,243,784,121	1.14%	40.4%
2013	2,712,239,573	8.0%	7,162,119,430	1.16%	37.9%
2012	2,511,615,523	10.5%	7,080,072,420	1.17%	35.5%
2011	2,272,463,038	11.7%	6,997,998,760	1.18%	32.5%
2010	2,034,259,368	16.1%	6,916,183,480	1.19%	29.4%
2009	1,752,333,178	12.2%	6,834,721,930	1.20%	25.6%
2008	1,562,067,594	13.8%	6,753,649,230	1.21%	23.1%
2007	1,373,040,542	18.6%	6,673,105,940	1.21%	20.6%
2006	1,157,500,065	12.4%	6,593,227,980	1.21%	17.6%
2005	1,029,717,906	13.1%	6,514,094,610	1.22%	15.8%
2004	910,060,180	16.9%	6,435,705,600	1.22%	14.1%
2003	778,555,680	17.5%	6,357,991,750	1.23%	12.2%
2002	662,663,600	32.4%	6,280,853,820	1.24%	10.6%
2001	500,609,240	21.1%	6,204,147,030	1.25%	8.1%
2000	413,425,190	47.2%	6,127,700,430	1.26%	6.7%
1999	280,866,670	49.4%	6,051,478,010	1.27%	4.6%
1998	188,023,930	55.7%	5,975,303,660	1.30%	3.1%
1997	120,758,310	56.0%	5,898,688,340	1.33%	2.0%
1996	77,433,860	72.7%	5,821,016,750	1.38%	1.3%
1995	44,838,900	76.2%	5,741,822,410	1.43%	0.8%
1994	25,454,590	79.7%	5,661,086,350	1.47%	0.4%
1993	14,161,570		5,578,865,110		0.3%

INTERNET USERS BY REGION



INTERNET USERS BY COUNTRY

In 2014, nearly 75% (2.1 billion) of all internet users in the world (2.8 billion) live in the top 20 countries.

The remaining 25% (0.7 billion) is distributed among the other 178 countries, each representing less than 1% of total users.

China, the country with most users (642 million in 2014), represents nearly 22% of total, and has more users than the next three countries combined (United States, India, and Japan). Among the top 20 countries, India is the one with the lowest penetration: 19% and the highest yearly growth rate. At the opposite end of the range, United States, Germany, France, U.K., and Canada have the highest penetration: over 80% of population in these countries has an internet connection.

LIST OF COUNTRIES BY INTERNET USAGE (2014)

List of Countries by Internet Usage (2014)

Show 10 entries   Search:

Rank	Country	Internet Users	1 Year Growth %	1 Year User Growth	Total Country Population	1 Yr Population Change (%)	Penetration (% of Pop. with Internet)	Country's share of World Population	Country's share of World Internet Users
1	China	641,601,070	4%	24,021,070	1,393,783,836	0.59%	46.03%	19.24%	21.97%
2	United States	279,834,232	7%	17,754,869	322,583,006	0.79%	86.75%	4.45%	9.58%
3	India	243,198,922	14%	29,859,598	1,267,401,849	1.22%	19.19%	17.50%	8.33%
4	Japan	109,252,912	8%	7,668,535	126,999,808	-0.11%	86.03%	1.75%	3.74%
5	Brazil	107,822,831	7%	6,884,333	202,033,670	0.83%	53.37%	2.79%	3.69%
6	Russia	84,437,793	10%	7,494,536	142,467,651	-0.26%	59.27%	1.97%	2.89%
7	Germany	71,727,551	2%	1,525,829	82,652,256	-0.09%	86.78%	1.14%	2.46%
8	Nigeria	67,101,452	16%	9,365,590	178,516,904	2.82%	37.59%	2.46%	2.30%
9	United Kingdom	57,075,826	3%	1,574,653	63,489,234	0.56%	89.90%	0.88%	1.95%
10	France	55,429,382	3%	1,521,369	64,641,279	0.54%	85.75%	0.89%	1.90%

Showing 1 to 10 of 198 entries   Previous 1 2 3 4 5 ... 20 Next

View Full Table

Source: *Internet Live Stats* (www.InternetLiveStats.com)

Elaboration of data by *International Telecommunication Union (ITU), United Nations Population Division, Internet & Mobile Association of India (IAMAI), World Bank.*

July 1 2014 Estimate

DEFINITIONS:

USER

An individual who has access to the Internet at home. This indicator does not record use, or frequency of use, but only access. In order to have access, the hardware equipment must be in working conditions, the Internet subscription service must be active, and the individual household member must have access to it at any time (there must be no barriers preventing the individual from using the Internet). The hardware equipment may or may not be owned by the household. There are no age limits (minimum or maximum), so an Internet user can be of any age. There can be multiple devices and services within the household. The data is collected through annual household surveys administered by individual countries based on ITU guidelines.[1] The United Nations Statistics Division has recommended collection of data on households accessing the Internet also outside of home [2], but this is not a Core ICT Indicator. [3] An "Internet User" is therefore defined as an individual who can access the Internet, via computer or mobile device, within the home where the individual lives.

INTERNET

A world-wide computer network that can be accessed via a computer, mobile telephone, PDA, games machine, digital TV, etc. The Internet access service can be provided through a fixed (wired) or mobile network: analogue dial-up modem via standard telephone line, ISDN (Integrated Services Digital Network), DSL (Digital Subscriber Line) or ADSL, Cable modem, High speed leased lines, Fiber, Powerline, Satellite broadband network, WiMAX, Fixed

CDMA, Mobile broadband network (3G, e.g. UMTS) via a handset or card, Integrated SIM card in a computer, or USB modem.

SOURCES

Current internet user population estimates are delivered by Worldometers' RTS algorithm, which processes data elaborated through statistical analysis after being collected from the following sources:

International Telecommunication Union (ITU) - United Nations specialized agency for information and communication technologies and the official source for global ICT statistics The World in 2014: ICT Facts and Figures – ITU Measuring the Information Society - ITU MIS Report 2013 Internet Users Data - World Bank Group The World Factbook: Internet Users - U.S. Central Intelligence Agency United Nations Population Division - U.N. Department of Economic and Social Affairs.

REFERENCES

1- Manual for Measuring ICT Access and Use by Households and Individuals, 2014. International Telecommunication Union (ITU).

2- 2010 World Population and Housing Census Programme. United Nations Statistics Division (UNSD)

3- Core ICT Indicators 2010. International Telecommunication Union (ITU).

1	China	641,601,070	4%	24,021,070	1,393,783,836	0.59%	46.03%	19.24%	21.97%
2	United States	279,834,232	7%	17,754,869	322,583,006	0.79%	86.75%	4.45%	9.58%
3	India	243,198,922	14%	29,859,598	1,267,401,849	1.22%	19.19%	17.50%	8.33%
4	Japan	109,252,912	8%	7,668,535	126,999,808	-0.11%	86.03%	1.75%	3.74%
5	Brazil	107,822,831	7%	6,884,333	202,033,670	0.83%	53.37%	2.79%	3.69%
6	Russia	84,437,793	10%	7,494,536	142,467,651	-0.26%	59.27%	1.97%	2.89%
7	Germany	71,727,551	2%	1,525,829	82,652,256	-0.09%	86.78%	1.14%	2.46%
8	Nigeria	67,101,452	16%	9,365,590	178,516,904	2.82%	37.59%	2.46%	2.30%
9	United Kingdom	57,075,826	3%	1,574,653	63,489,234	0.56%	89.90%	0.88%	1.95%
10	France	55,429,382	3%	1,521,369	64,641,279	0.54%	85.75%	0.89%	1.90%
11	Mexico	50,923,060	7%	3,423,153	123,799,215	1.20%	41.13%	1.71%	1.74%
12	South Korea	45,314,248	8%	3,440,213	49,512,026	0.51%	91.52%	0.68%	1.55%

13	Indonesia	42,258,824	9%	3,468,057	252,812,245	1.18%	16.72%	3.49%	1.45%
14	Egypt	40,311,562	10%	3,748,271	83,386,739	1.62%	48.34%	1.15%	1.38%
15	Viet Nam	39,772,424	9%	3,180,007	92,547,959	0.95%	42.97%	1.28%	1.36%
16	Philippines	39,470,845	10%	3,435,654	100,096,496	1.73%	39.43%	1.38%	1.35%
17	Italy	36,593,969	2%	857,489	61,070,224	0.13%	59.92%	0.84%	1.25%
18	Turkey	35,358,888	3%	1,195,610	75,837,020	1.21%	46.62%	1.05%	1.21%
19	Spain	35,010,273	3%	876,986	47,066,402	0.30%	74.38%	0.65%	1.20%
20	Canada	33,000,381	7%	2,150,061	35,524,732	0.98%	92.89%	0.49%	1.13%
21	Poland	25,666,238	2%	571,136	38,220,543	0.01%	67.15%	0.53%	0.88%
22	Colombia	25,660,725	7%	1,739,108	48,929,706	1.26%	52.44%	0.68%	0.88%
23	Argentina	24,973,660	7%	1,600,722	41,803,125	0.86%	59.74%	0.58%	0.86%
24	South Africa	24,909,854	14%	3,022,362	53,139,528	0.69%	46.88%	0.73%	0.85%
25	Iran	22,200,708	9%	1,850,445	78,470,222	1.32%	28.29%	1.08%	0.76%
26	Australia	21,176,595	9%	1,748,054	23,630,169	1.23%	89.62%	0.33%	0.73%
27	Morocco	20,207,154	10%	1,851,335	33,492,909	1.47%	60.33%	0.46%	0.69%
28	Pakistan	20,073,929	9%	1,731,250	185,132,926	1.64%	10.84%	2.56%	0.69%
29	Thailand	19,386,154	8%	1,438,018	67,222,972	0.32%	28.84%	0.93%	0.66%
30	Saudi Arabia	17,397,179	11%	1,656,942	29,369,428	1.88%	59.24%	0.41%	0.60%
31	Madagascar	17,321,756	16%	2,417,590	23,571,962	2.82%	73.48%	0.33%	0.59%
32	Ukraine	16,849,008	9%	1,433,455	44,941,303	-0.66%	37.49%	0.62%	0.58%
33	Kenya	16,713,319	16%	2,313,820	45,545,980	2.69%	36.70%	0.63%	0.57%
34	Netherlands	16,143,879	3%	398,245	16,802,463	0.26%	96.08%	0.23%	0.55%
35	Venezuela	14,548,421	7%	1,013,852	30,851,343	1.47%	47.16%	0.43%	0.50%
36	Peru	12,583,953	7%	857,081	30,769,077	1.30%	40.90%	0.42%	0.43%
37	Malawi	12,150,362	16%	1,698,742	16,829,144	2.85%	72.20%	0.23%	0.42%
38	Uzbekistan	11,914,665	12%	1,229,670	29,324,920	1.35%	40.63%	0.40%	0.41%
39	Mali	11,862,559	16%	1,678,081	15,768,227	3.05%	75.23%	0.22%	0.41%
40	Chile	11,686,746	7%	749,968	17,772,871	0.87%	65.76%	0.25%	0.40%
41	Romania	11,178,477	2%	218,123	21,640,168	-0.27%	51.66%	0.30%	0.38%
42	Bangladesh	10,867,567	9%	896,332	158,512,570	1.22%	6.86%	2.19%	0.37%
43	Kazakhstan	9,850,123	11%	986,929	16,606,878	1.01%	59.31%	0.23%	0.34%
44	Belgium	9,441,116	3%	242,233	11,144,420	0.36%	84.72%	0.15%	0.32%
45	Sudan	9,307,189	15%	1,242,839	38,764,090	2.11%	24.01%	0.54%	0.32%

46	United Arab Emirates	8,807,226	10%	774,914	9,445,624	1.06%	93.24%	0.13%	0.30%
47	Sweden	8,581,261	1%	110,156	9,631,261	0.63%	89.10%	0.13%	0.29%
48	Czech Republic	8,322,168	3%	213,353	10,740,468	0.36%	77.48%	0.15%	0.28%
49	Tanzania	7,590,794	16%	1,074,118	50,757,459	3.05%	14.96%	0.70%	0.26%
50	Hungary	7,388,776	2%	147,846	9,933,173	-0.22%	74.38%	0.14%	0.25%
51	Switzerland	7,180,749	3%	227,983	8,157,896	0.99%	88.02%	0.11%	0.25%
52	Austria	7,135,168	3%	183,661	8,526,429	0.37%	83.68%	0.12%	0.24%
53	Portugal	7,015,519	2%	156,800	10,610,304	0.02%	66.12%	0.15%	0.24%
54	Algeria	6,669,927	10%	633,077	39,928,947	1.84%	16.70%	0.55%	0.23%
55	Uganda	6,523,949	17%	940,168	38,844,624	3.37%	16.79%	0.54%	0.22%
56	Greece	6,438,325	2%	142,859	11,128,404	0.00%	57.85%	0.15%	0.22%
57	Ecuador	6,012,003	8%	423,777	15,982,551	1.55%	37.62%	0.22%	0.21%
58	Israel	5,928,772	3%	197,273	7,822,107	1.15%	75.80%	0.11%	0.20%
59	Syria	5,860,788	9%	480,524	21,986,615	0.40%	26.66%	0.30%	0.20%
60	Hong Kong SAR	5,751,357	9%	450,747	7,259,569	0.77%	79.22%	0.10%	0.20%
61	Azerbaijan	5,737,223	11%	578,231	9,514,887	1.08%	60.30%	0.13%	0.20%
62	Denmark	5,419,113	3%	139,859	5,640,184	0.38%	96.08%	0.08%	0.19%
63	Ghana	5,171,993	15%	689,264	26,442,178	2.08%	19.56%	0.37%	0.18%
64	Finland	5,117,660	3%	129,157	5,443,497	0.32%	94.01%	0.08%	0.18%
65	Dominican Republic	5,072,674	7%	341,197	10,528,954	1.20%	48.18%	0.15%	0.17%
66	Tunisia	5,053,704	10%	446,032	11,116,899	1.09%	45.46%	0.15%	0.17%
67	Norway	4,895,885	2%	105,347	5,091,924	0.98%	96.15%	0.07%	0.17%
68	Belarus	4,856,969	9%	419,164	9,307,609	-0.52%	52.18%	0.13%	0.17%
69	Yemen	4,778,488	11%	473,030	24,968,508	2.30%	19.14%	0.34%	0.16%
70	Serbia	4,705,141	2%	83,759	9,468,378	-0.44%	49.69%	0.13%	0.16%
71	Slovakia	4,507,849	2%	103,037	5,454,154	0.07%	82.65%	0.08%	0.15%
72	Singapore	4,453,859	10%	396,302	5,517,102	1.95%	80.73%	0.08%	0.15%
73	Angola	4,286,821	17%	608,233	22,137,261	3.10%	19.36%	0.31%	0.15%
74	Sri Lanka	4,267,507	9%	335,915	21,445,775	0.81%	19.90%	0.30%	0.15%
75	New Zealand	4,162,209	9%	85,828	4,551,349	1.01%	91.45%	0.06%	0.14%
76	Bulgaria	4,083,950	1%	59,858	7,167,998	0.76%	56.97%	0.10%	0.14%
77	Bolivia	3,970,587	8%	283,474	10,847,664	1.65%	36.60%	0.15%	0.14%
78	Ireland	3,817,491	3%	124,604	4,677,340	1.08%	81.62%	0.06%	0.13%

79	Nepal	3,411,948	9%	279,504	28,120,740	1.16%	12.13%	0.39%	0.12%
80	Jordan	3,375,307	12%	359,976	7,504,812	3.18%	44.98%	0.10%	0.12%
81	Lebanon	3,336,517	12%	350,316	4,965,914	2.99%	67.19%	0.07%	0.11%
82	Senegal	3,194,190	16%	448,824	14,548,171	2.94%	21.96%	0.20%	0.11%
83	Cuba	3,090,796	6%	171,379	11,258,597	-0.06%	27.45%	0.16%	0.11%
84	Kuwait	3,022,010	12%	325,256	3,479,371	3.29%	86.86%	0.05%	0.10%
85	Zimbabwe	2,852,757	17%	406,610	14,599,325	3.18%	19.54%	0.20%	0.10%
86	Croatia	2,780,534	2%	50,350	4,272,044	-0.41%	65.09%	0.06%	0.10%
87	Guatemala	2,716,781	9%	215,550	15,859,714	2.53%	17.13%	0.22%	0.09%
88	Iraq	2,707,928	12%	284,010	34,768,761	2.97%	7.79%	0.48%	0.09%
89	Oman	2,584,316	17%	380,679	3,926,492	8.10%	65.82%	0.05%	0.09%
90	Bosnia Herzegovina	2,582,502	2%	54,197	3,824,746	-0.12%	67.52%	0.05%	0.09%
91	Costa Rica	2,511,139	7%	172,205	4,937,755	1.35%	50.86%	0.07%	0.09%
92	Zambia	2,313,013	17%	332,362	15,021,002	3.32%	15.40%	0.21%	0.08%
93	Qatar	2,191,866	13%	259,980	2,267,916	4.58%	96.65%	0.03%	0.08%
94	Georgia	2,188,311	10%	191,034	4,322,842	-0.42%	50.62%	0.06%	0.07%
95	Lithuania	2,113,393	2%	40,877	3,008,287	-0.29%	70.25%	0.04%	0.07%
96	Puerto Rico	2,027,549	6%	111,168	3,683,601	-0.13%	55.04%	0.05%	0.07%
97	Uruguay	2,017,280	6%	119,523	3,418,694	0.34%	59.01%	0.05%	0.07%
98	Paraguay	2,005,278	8%	143,917	6,917,579	1.69%	28.99%	0.10%	0.07%
99	Panama	1,899,892	8%	134,718	3,926,017	1.60%	48.39%	0.05%	0.07%
100	Afghanistan	1,856,781	10%	172,462	31,280,518	2.39%	5.94%	0.43%	0.06%
101	Albania	1,798,686	3%	46,550	3,185,413	0.38%	56.47%	0.04%	0.06%
102	El Salvador	1,742,832	7%	108,823	6,383,752	0.68%	27.30%	0.09%	0.06%
103	Ethiopia	1,636,099	16%	224,689	96,506,031	2.56%	1.70%	1.33%	0.06%
104	Honduras	1,602,558	8%	119,664	8,260,749	2.01%	19.40%	0.11%	0.05%
105	Latvia	1,560,452	2%	27,686	2,041,111	-0.45%	76.45%	0.03%	0.05%
106	Moldova	1,550,925	2%	23,042	3,461,380	-0.74%	44.81%	0.05%	0.05%
107	Slovenia	1,501,039	2%	35,794	2,075,592	0.17%	72.32%	0.03%	0.05%
108	Cameroon	1,486,815	16%	203,954	22,818,632	2.54%	6.52%	0.32%	0.05%
109	Mozambique	1,467,687	16%	200,551	26,472,977	2.47%	5.54%	0.37%	0.05%
110	Jamaica	1,393,381	7%	85,107	2,798,837	0.54%	49.78%	0.04%	0.05%
111	Libya	1,362,604	9%	117,091	6,253,452	0.84%	21.79%	0.09%	0.05%

112	Kyrgyzstan	1,359,416	12%	140,850	5,625,015	1.40%	24.17%	0.08%	0.05%
113	Tajikistan	1,357,400	13%	153,157	8,408,947	2.45%	16.14%	0.12%	0.05%
114	Armenia	1,300,013	10%	121,362	2,983,990	0.25%	43.57%	0.04%	0.04%
115	Bahrain	1,297,500	9%	112,188	1,344,111	0.90%	96.53%	0.02%	0.04%
116	Haiti	1,217,505	7%	84,040	10,461,409	1.40%	11.64%	0.14%	0.04%
117	Rwanda	1,110,043	16%	154,226	12,100,049	2.75%	9.17%	0.17%	0.04%
118	Estonia	1,047,772	2%	20,433	1,283,771	-0.27%	81.62%	0.02%	0.04%
119	Nicaragua	891,675	7%	62,082	6,169,269	1.46%	14.45%	0.09%	0.03%
120	Trinidad and Tobago	856,544	6%	49,854	1,344,235	0.23%	63.72%	0.02%	0.03%
121	Cambodia	828,317	10%	72,646	15,408,270	1.80%	5.38%	0.21%	0.03%
122	Burkina Faso	741,888	16%	103,792	17,419,615	2.86%	4.26%	0.24%	0.03%
123	Cyprus	726,663	3%	23,426	1,153,058	1.04%	63.02%	0.02%	0.02%
124	Malaysia	675,074	9%	57,875	30,187,896	1.58%	2.24%	0.42%	0.02%
125	Myanmar	624,991	9%	49,496	53,718,958	0.86%	1.16%	0.74%	0.02%
126	Côte d›Ivoire	565,874	16%	76,995	20,804,774	2.41%	2.72%	0.29%	0.02%
127	Mongolia	514,254	9%	43,655	2,881,415	1.49%	17.85%	0.04%	0.02%
128	Luxembourg	510,177	3%	17,232	536,761	1.20%	95.05%	0.01%	0.02%
129	Benin	460,232	16%	63,660	10,599,510	2.67%	4.34%	0.15%	0.02%
130	Mauritania	455,553	16%	62,084	3,984,457	2.43%	11.43%	0.06%	0.02%
131	Turkmenistan	424,855	11%	43,584	5,307,171	1.28%	8.01%	0.07%	0.01%
132	Montenegro	364,978	2%	8,176	621,542	0.03%	58.72%	0.01%	0.01%
133	Namibia	347,414	15%	45,898	2,347,988	1.94%	14.80%	0.03%	0.01%
134	Fiji	325,717	8%	25,238	887,027	0.68%	36.72%	0.01%	0.01%
135	Iceland	321,475	1%	4,133	333,135	1.09%	96.50%	0.00%	0.01%
136	Togo	319,822	16%	44,001	6,993,244	2.59%	4.57%	0.10%	0.01%
137	Chad	317,197	16%	44,763	13,211,146	3.01%	2.40%	0.18%	0.01%
138	Martinique	303,302	6%	17,720	404,705	0.25%	74.94%	0.01%	0.01%
139	Swaziland	301,211	15%	38,548	1,267,704	1.46%	23.76%	0.02%	0.01%
140	Niger	298,310	17%	44,407	18,534,802	3.95%	1.61%	0.26%	0.01%
141	Guyana	295,200	6%	17,951	803,677	0.51%	36.73%	0.01%	0.01%
142	Bahamas	293,875	7%	20,236	382,571	1.38%	76.82%	0.01%	0.01%
143	Brunei	277,589	9%	23,078	423,205	1.30%	65.59%	0.01%	0.01%
144	Gambia	271,711	17%	38,837	1,908,954	3.23%	14.23%	0.03%	0.01%

145	Botswana	268,038	14%	32,929	2,038,587	0.86%	13.15%	0.03%	0.01%
146	Barbados	224,588	6%	13,639	286,066	0.50%	78.51%	0.00%	0.01%
147	Bhutan	211,896	9%	18,079	765,552	1.54%	27.68%	0.01%	0.01%
148	Guinea	205,194	16%	28,158	12,043,898	2.54%	1.70%	0.17%	0.01%
149	Suriname	201,963	7%	12,947	543,925	0.86%	37.13%	0.01%	0.01%
150	Cape Verde	200,060	14%	24,729	503,637	0.95%	39.72%	0.01%	0.01%
151	Liberia	190,731	16%	25,933	4,396,873	2.39%	4.34%	0.06%	0.01%
152	Papua New Guinea	187,284	10%	16,945	7,476,108	2.12%	2.51%	0.10%	0.01%
153	Malta	173,003	3%	4,282	430,146	0.27%	40.22%	0.01%	0.01%
154	Gabon	168,592	16%	22,886	1,711,294	2.37%	9.85%	0.02%	0.01%
155	New Caledonia	163,997	9%	13,634	259,824	1.30%	63.12%	0.00%	0.01%
156	Somalia	163,185	12%	17,090	10,805,651	2.95%	1.51%	0.15%	0.01%
157	Central African Republic	161,524	15%	21,436	4,709,203	2.01%	3.43%	0.07%	0.01%
158	French Polynesia	161,025	9%	13,077	279,835	1.09%	57.54%	0.00%	0.01%
159	Burundi	146,219	17%	20,808	10,482,752	3.15%	1.39%	0.14%	0.01%
160	Equatorial Guinea	124,035	16%	17,267	778,061	2.78%	15.94%	0.01%	0.00%
161	Guam	112,196	9%	9,499	167,546	1.47%	66.96%	0.00%	0.00%
162	Lesotho	110,065	14%	13,758	2,097,511	1.11%	5.25%	0.03%	0.00%
163	Mayotte	107,940	16%	14,921	228,070	2.66%	47.33%	0.00%	0.00%
164	Sierra Leone	92,232	15%	12,123	6,205,382	1.86%	1.49%	0.09%	0.00%
165	Belize	90,939	8%	7,081	339,758	2.37%	26.77%	0.00%	0.00%
166	Congo	87,559	16%	11,980	4,558,594	2.49%	1.92%	0.06%	0.00%
167	Aruba	81,945	6%	4,981	103,431	0.51%	79.23%	0.00%	0.00%
168	Antigua and Barbuda	81,545	7%	5,347	90,903	1.02%	89.71%	0.00%	0.00%
169	Djibouti	80,378	10%	7,410	886,313	1.53%	9.07%	0.01%	0.00%
170	Mauritius	76,681	13%	9,098	1,249,151	0.38%	6.14%	0.02%	0.00%
171	Andorra	71,575	3%	2,402	80,153	1.18%	89.30%	0.00%	0.00%
172	Bermuda	63,987	6%	3,696	65,461	0.18%	97.75%	0.00%	0.00%
173	Eritrea	59,784	17%	8,535	6,536,176	3.21%	0.91%	0.09%	0.00%
174	Guinea-Bissau	57,764	16%	7,875	1,745,798	2.44%	3.31%	0.02%	0.00%
175	Seychelles	50,220	14%	6,012	93,306	0.50%	53.82%	0.00%	0.00%
176	Comoros	49,320	11%	4,919	752,438	2.38%	6.55%	0.01%	0.00%
177	Sao Tome and Principe	48,806	16%	6,693	197,882	2.53%	24.66%	0.00%	0.00%

178	Grenada	47,903	6%	2,857	106,303	0.38%	45.06%	0.00%	0.00%
179	Cayman Islands	47,003	7%	3,227	59,226	1.35%	79.36%	0.00%	0.00%
180	Solomon Islands	43,623	10%	3,931	572,865	2.07%	7.61%	0.01%	0.00%
181	Faeroe Islands	43,605	2%	958	49,460	-0.02%	88.16%	0.00%	0.00%
182	Dominica	42,735	6%	2,583	72,341	0.47%	59.07%	0.00%	0.00%
183	Tonga	40,131	8%	3,021	105,782	0.44%	37.94%	0.00%	0.00%
184	Greenland	39,717	6%	2,342	57,164	0.31%	69.48%	0.00%	0.00%
185	Liechtenstein	34,356	3%	1,004	37,194	0.73%	92.37%	0.00%	0.00%
186	Monaco	34,214	3%	964	38,066	0.62%	89.88%	0.00%	0.00%
187	Vanuatu	29,791	10%	2,716	258,301	2.19%	11.53%	0.00%	0.00%
188	Micronesia	29,370	8%	2,185	103,903	0.34%	28.27%	0.00%	0.00%
189	Samoa	26,977	8%	2,112	191,831	0.77%	14.06%	0.00%	0.00%
190	Maldives	16,645	10%	1,474	351,572	1.90%	4.73%	0.00%	0.00%
191	San Marino	16,631	3%	466	31,637	0.60%	52.57%	0.00%	0.00%
192	Kiribati	12,156	9%	1,039	103,942	1.55%	11.70%	0.00%	0.00%
193	Timor-Leste	11,472	10%	998	1,152,439	1.73%	1.00%	0.02%	0.00%
194	Caribbean Netherlands	10,233	8%	769	19,525	2.06%	52.41%	0.00%	0.00%
195	Tuvalu	3,768	8%	275	9,894	0.18%	38.09%	0.00%	0.00%
196	Cook Islands	1,378	8%	105	20,732	0.50%	6.65%	0.00%	0.00%
197	Marshall Islands	1,246	8%	92	52,772	0.26%	2.36%	0.00%	0.00%
198	Niue	617	5%	28	1,307	-2.75%	47.20%	0.00%	0.00%

ملحق رقم (٤)

إحصائية مستخدمي الأنترنت

في دول مجلس التعاون لدول الخليج العربية

إحصائية مستخدمي الأنترنت في دول مجلس التعاون لدول الخليج العربية

ت	الدولة	الترتيب العالمي	عدد مستخدمي الانترنت	نسبة النمو السنوي	النمو السنوي للمستخدمين	عدد السكان	النمو السكاني السنوي	نسبة المستخدمين الى عدد السكان	نسبة السكان الى عدد سكان العالم	نسبة المستخدمين الى العدد الكلي من العالم
-١	المملكة العربية السعودية	٣٠	١٧,٣٩٧,١٧٩	11%	١,٦٥٦,٩٤٢	٢٩,٣٦٩,٤٢٨	1.88%	59.24%	0.41%	0.60%
-٢	دولة الامارات العربية المتحدة	٤٦	٨,٨٠٧,٢٢٦	10%	٧٧٤,٩١٩	٩,٤٤٥,٦٢٤	1.06%	٩٣,٢٤%	٠,١٣%	٠,٣٠%
-٣	الكـــويـــت	٨٤	٣,٠٢٢,٠١٠	12%	٣٢٥,٢٢٦	٣,٤٧٩,٣٧١	٣,٢٩%	86.86%	٠,٠٥%	٠,١٠%
-٤	سلطنة عمان	٨٩	٢,٥٨٤,١٣٦	17%	٣٨٠,٦٧٩	٣,٩٢٦,٤٩٢	8.10%	65.82%	٠,٠٥%	٠,٣٠%
-٥	قــطـــــر	٩٣	٢,١٩١,٨٦٦	13%	٢٥٩,٩٨٠	٢,٢٦٧,٩١٦	4.58%	96.65%	٠,٠٣%	٠,٠٨%
-٦	البحــرين	١١٥	١,٢٩٧,٥٠٠	9%	١١٢,١٨٨	١,٣٤٤,١١١	0.90%	96.53%	٠,٠٢%	٠,٠١%

Source: Internet live stats (www.internetlivestats.com).

Elaboration of data by international telecommunication union (ITU), United nations Population Division internet & Mobile Association y India (IAMAI), July Estimate World Bank.

Internet User = Individual, at any age who can access the internet home by device type (Computer or Mobile) and connection.

Internet live stats has been cited by: The official world wide web anniversary site world wed consortium (w3c)

Word wid wed Foundaion



ملحق رقم (٥)

إحصائيات الجريمة الاليكترونية

من ب ـ و

يشتمل الملحق على احصائيات الجريمة الاليكترونية التالية :

- التقديرات السنوية للحماية من الجريمة الاليكترونية تبلغ ١٠٠ مليار دولار ومن المتوقع وصولها الي ١٢٠ مليار في عام ٢٠١٧.

- تقديرات ضحايا الجريمة الاليكترونية سنويا:

٥٥٦ مليون ضحية كل عام - ١,٥ مليون ضحية كل يوم – ١٨ ضحية في الثانية – ٢٣٢,٤ مليون بطاقة هوية تتم سرقة معلوماتها – أكثر من ٦٠٠ألف حساب في الفيس بوك الاشتباه فيها والاطلاع عليها يوميا – ١من كل ١٠ أشخاص من مستخدمي شبكات التواصل الاجتماعي يقعون ضحية لتواصل مشبوه ز

- أنواع الهجمات الإلكترونية المعتادة .

- احصائية ضحايا الجريمة الإلكترونية حسب الجنس (Gender)

- احصائية الحصول غير المشروع على بيانات مؤسسات القطاع العام والخاص .

- احصائية حالات الاحتيال على المصارف.

- احصائية ال١٥ دولة الاولى التي تنطلق منها هجمات الجريمة الاليكترونية .

68%0,7 48(5<
$// EORJ SKS (FRPPHUFH KWWS ZZZ JR JXOI FRP EORJ FDWHJRU\ HFRPPHUFH ,QWHUQHW KWWS ZZZ JR
JXOI FRP EORJ FDWHJRU\ LQWHUQHW ,QWHUYLHZV KWWS ZZZ JR JXOI FRP EORJ FDWHJRU\ LQWHUYLHZV ,QWUDQHW KWWS ZZZ JR
JXOI FRP EORJ FDWHJRU\ LQWUDQHW EORJ 6(2 6(0 KWWS ZZZ JR JXOI FRP EORJ FDWHJRU\ VHR VHP 6RFLDO 0HGLD KWWS ZZZ JR
JXOI FRP EORJ FDWHJRU\ VRFLDO PHGLD :HE 'HVLJQ KWWS ZZZ JR JXOI FRP EORJ FDWHJRU\ ZHE GHVLJQ
%/2*
/LNH
0$<
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH
&\EHU &ULPHV DUH JURZLQJ DQG E\ WKH JOREDO &\EHU 6HFXULW\ PDUNHW LV H[SHFWHG WR VN\URFNHW WR
ELOOLRQ 7KH HVWLPDWHG DQQXDO FRVW RYHU JOREDO F\EHU FULPH LV ELOOLRQ &KHFN RXW RXU
LQIRJUDSKLF WR NQRZ WKH ODWHVW VWDWLVWLFV DQG WUHQGV RI &\EHU &ULPH LQGXVWU\
7ZHHW .H\ZRUG
5(&(17 32676
0' 3URSHUWLHV :LQ 7RS $ZDUG
³%HVW 5HDO (VWDWH $JHQF\ 4DWDU
$ZDUG´ KWWS ZZZ JR
JXOI FRP EORJ PG SURSHUWLHV ZLQ
WRS DZDUG EHVW UHDO HVWDWH
DJHQF\ TDWDU DZDUG
+RZ 0XFK 'R 6PDUWSKRQHV
&RVW 6WDWLVWLFV DQG 7UHQGV
KWWS ZZZ JR
JXOI FRP EORJ VPDUWSKRQHV FRVW
7HVWLQJ \RXU UHVSRQVLYH ZHE
GHVLJQ ZLWK *RRJOH DQDO\WLFV
KWWS ZZZ JR
JXOI FRP EORJ WHVWLQJ UHVSRQVLYH
ZHE GHVLJQ
,QWHUYLHZ :LWK)RXQGHUV RI
0LGGOH (DVW 6WDUW 8S :HSXO
KWWS ZZZ JR
JXOI FRP EORJ LQWHUYLHZ ZLWK
IRXQGHUV ZHSXO
0LGGOH (DVW 6WDUWXSV <RX
6KRXOG .QRZ $ERXW
KWWS ZZZ JR
JXOI FRP EORJ PLGGOH HDVW
VWDUWXSV \RX VKRXOG NQRZ

DERXW
KWWS ZZZ JR
JXOI FRP
+20(+773 ::: *2 *8/) &20 6(59,&(6 +773 ::: *2 *8/) &20 6(59,&(6 3+3
62/87,216 +773 ::: *2 *8/) &20 62/87,216 3+3
3257)2/,2 +773 ::: *2 *8/) &20 3257)2/,2 3+3
&203$1< +773 ::: *2 *8/) &20 &203$1< 3+3
35,&,1* &217$&7 +773 ::: *2 *8/) &20 (148,5< 3+3
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ 3DJH RI
KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH -DQ
)HDWXUHG ,Q
KWWS ZZZ JR
JXOI FRP EORJ SXEOLFDWLRQV
PHQWLRQHG JR JXOI
6XEVFULEH \RXU HPDLO
(QWHU HPDLO
68%0,7
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ 3DJH RI
KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH -DQ
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ 3DJH RI
KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH -DQ
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ 3DJH RI
KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH -DQ
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ 3DJH RI
KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH -DQ
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ 3DJH RI
KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH -DQ
KWWS ZZZ JR JXOI FRP ZS FRQWHQW XSORDGV F\EHU FULPH MSJ
,QIRJUDSKLF E\ *2 *XOI KWWS ZZZ JR JXOI FRP
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ 3DJH RI
KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH -DQ
,QGXVWU\
0HGLFDO +HDOWKFDUH
%XVLQHVV
(GXFDWLRQDO
*RYHUQPHQW 0LOLWDU\
%DQNLQJ &UHGLW)LQDQFLDO
7R 3XEOLVK WKLV ,PDJH RQ \RXU %ORJ RU :HEVLWH &RS\ WKLV FRGH
D KUHI KWWS ZZZ JR JXOI FRP ZS FRQWHQW XSORDGV F\EHU FULPH MSJ ! LPJ
VUF KWWS ZZZ JR JXOI FRP ZS FRQWHQW XSORDGV F\EHU FULPH MSJ DOW &\EHU
&ULPH 6WDWLVWLFV
DQG 7UHQGV ZLGWK ! D! EU !
<HDUO\ &\EHU &ULPH 9LFWLP &RXQW (VWLPDWH
9LFWLPV SHU \HDU PLOOLRQ
9LFWLPV SHU GD\ 2YHU PLOOLRQ
9LFWLPV SHU VHFRQG
,GHQWLWLHV H[SRVHG 0RUH WKDQ PLOOLRQ

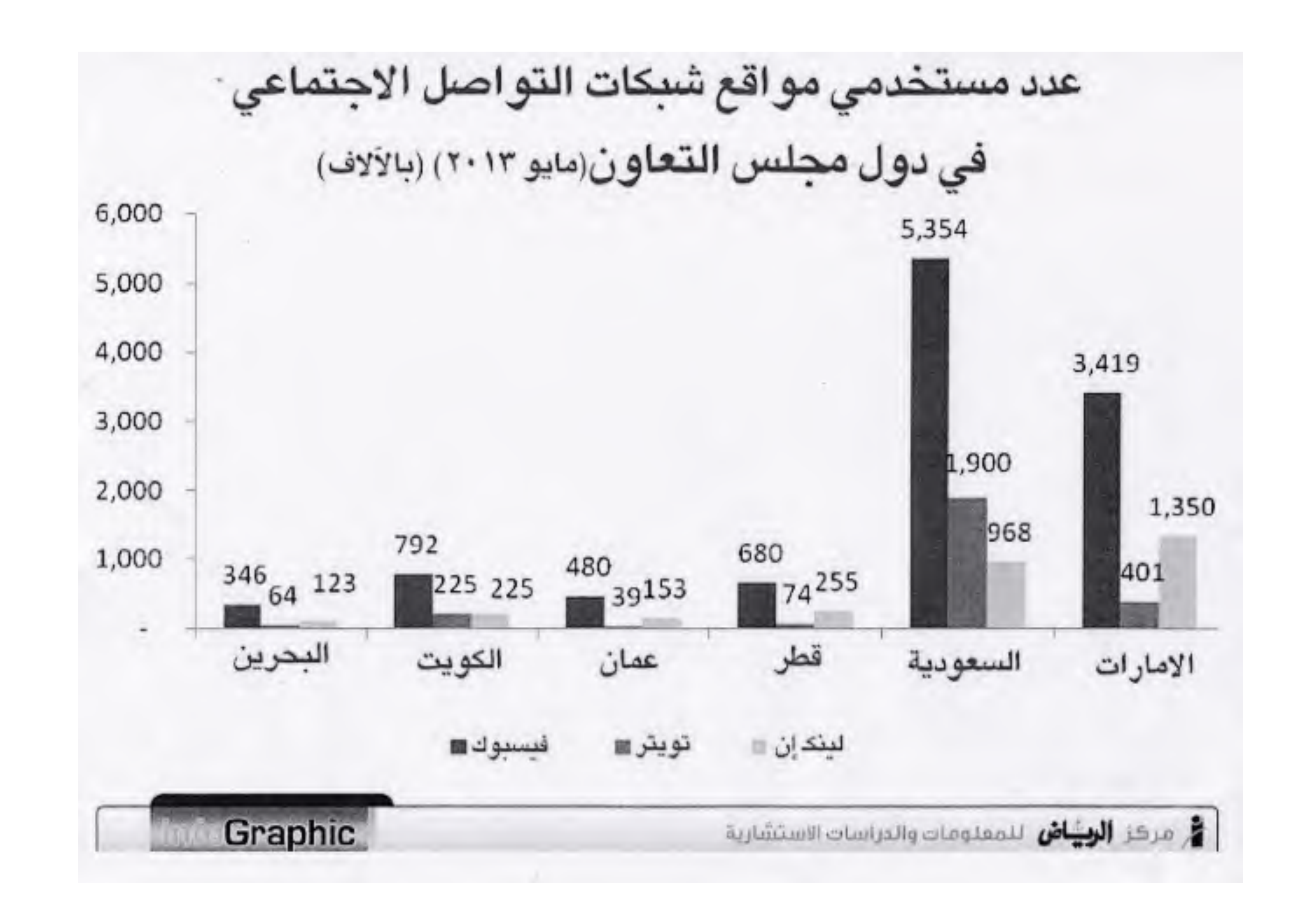
0RUH WKDQ)DFH%RRN DFFRXQWV DUH FRPSURPLVHG HYHU\ GD\
RI VRFLDO QHWZRUN XVHUV KDYH UHSRUWHG WKDW WKHLU SURILOHV KDYH EHHQ KDFNHG E\ SUHWHQGHUV
LQ VRFLDO QHWZRUN XVHUV VDLG WKH\×G IDOOHQ YLFWLP WR D VFDP RU IDNH OLQN RQ VRFLDO QHWZRUN SODWIRUPV
&RPPRQ 7\SHV 2I &\EHU $WWDFNV
$WWDFN 7\SHV
9LUXVHV PDOZDUH ZRUPV WURMDQV
&ULPLQDO LQVLGHU
7KHIW RI GDWD EHDULQJ GHYLFHV
64/ LQMHFWLRQ
3KLVKLQJ
:HE EDVHG DWWDFNV
6RFLDO HQJLQHHULQJ
2WKHU
%RWQHWV KDYH EHHQ XVLQJ DV PDQ\ DV LQIHFWHG Ù]RPELHÚFRPSXWHUV WR VHQG RXW VSDP HDFK
GD\
2I &\EHUFULPH 9LFWLPV %\ *HQGHU
*HQGHU DJH
0DOH
)HPDOHV
RI H[HPSOR\HHVDGPLWWHG WR VWHDOLQJ FRPSDQ\ GDWD ZKHQ OHDYLQJ SUHYLRXV MREV
'DWD %UHDFK 6WDWLVWLFV %\ ,QGXVWU\
7KH 0DMRU 0RWLYDWLRQ %HKLQG &\EHU $WWDFNV
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ 3DJH RI
KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH -DQ
b0RWLYDWLRQ)DFWRU
&\EHU &ULPH
+DFNWLYLVP
&\EHU :DUIDUH
&\EHU (VSLRQDJH
LV WKH XVH RI FRPSXWHUV DQG FRPSXWHU QHWZRUNV WR SURPRWH SROLWLFDO HQGV FKLHIO\ IUHH VSHHFK KXPDQ
ULJKWV DQG LQIRUPDWLRQ HWKLFV
b6WDWLVWLFV 2I %DQN)XQG)UDXG &DVHV /RVV $QG 5HFRYHU\
Ü ZHUH DEOH WR KROG RQ WR IXQGV
Ü ZHUH DEOH WR UHFRYHU IUDXGXOHQWO\ WUDQVIHUUHG IXQGV
Ü ZHUH GHFODUHG XQUHFRYHUDEOH
Ü FDXVHG ORVV WR EDQNV GXH WR UHLPEXUVHPHQWV
Ü FDXVHG ORVV WR EXVLQHVVHV
b&DXVHV)RU 2I 'LUHFW)LQDQFLDO &RVWV 2I &\EHU $WWDFNV ,Q 7KH 8 6
0DMRU 5HDVRQV
)UDXG
5HSDLUV
7KHIW RU /RVV

2WKHU
5XVVLD DQG WKH 8 6 DUH WKH ODUJHVW FRQWULEXWRUV ZKHQ LW FRPHV WR
PDOZDUH DWWDFNV PDNLQJ XS
DQG RI KRVWHG PDOZDUH UHVSHFWLYHO\
86 1DY\ VHHV F\EHU DWWDFNV HYHU\ KRXU RU PRUH WKDQ HYHU\ VLQJOH VHFRQG
7RS &RXQWULHV :KHUH &\EHU $WWDFNV 2ULJLQDWH)HEUXDU\
6RXUFH RI $WWDFN 1XPEHU RI $WWDFNV
5XVVLD
7DLZDQ
*HUPDQ\
8NUDLQH
+XQJDU\
86$
5RPDQLD
%UD]LO
,WDO\
$XVWUDOLD
$UJHQWLQD
&KLQD
3RODQG
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ 3DJH RI
KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH -DQ
0LGGOH (DVW ZHE GHVLJQ 0LGGOH (DVW ORJR GHVLJQ 0LGGOH (DVW 6(2
%ORJ KWWS ZZZ JR JXOI FRP EORJ SKS)$4 KWWS ZZZ JR JXOI FRP IDT SKS $IILOLDWHV
5HVHOOHUV KWWS ZZZ JR JXOI FRP DIILOLDWHV SKS
-RLQ XV KWWS ZZZ JR JXOI FRP MRLQXV SKS
k *2 *XOI $OO ULJKWV UHVHUYHG
:KDW 2XU &OLHQWV 6D\
$6)($785(' 21
/$7(67)520 7+(%/2*)$4
Ü 'R \RX ZRUN IRU FOLHQWV DEURDG" ,I \HV KRZ"
KWWS ZZZ JR JXOI FRP IDT SKS IDTB
Ü +RZ FDQ , UHYLHZ \RXU ZRUN VDPSOHV"
KWWS ZZZ JR JXOI FRP IDT SKS IDTB
Ü :KDW DUH \RXU SULFH UDQJHV DQG KRZ GR \RX FKDUJH"
KWWS ZZZ JR JXOI FRP IDT SKS IDTB
Ü +RZ PDQ\ GD\V GR \RX UHTXLUH WR GHYHORS D
ZHEVLWH" KWWS ZZZ JR JXOI FRP IDT SKS IDTB
Ü :KDW WHFKQRORJLHV GR \RX ZRUN ZLWK"
KWWS ZZZ JR JXOI FRP IDT SKS IDTB
Ü :KDW VHUYLFHV GR \RX RIIHU" KWWS ZZZ JR
JXOI FRP IDT SKS IDTB
Ü 'R \RX RSWLPL]H ZHEVLWHV IRU VHDUFK HQJLQHV 6(2 "
KWWS ZZZ JR JXOI FRP IDT SKS IDTB
Ü 'R \RX SURYLGH KRVWLQJ WRR" &DQ , XVH P\ SUHIHUUHG
ZHE KRVW EXW KDYH WKH VLWH EXLOW E\ \RX"
KWWS ZZZ JR JXOI FRP IDT SKS IDTB

Ü :KDW LI , ZDQW XSJUDGHV LQ WKH IXWXUH RU FKDQJHV WR D
ZHE SURMHFW WKDW KDV EHHQ GHYHORSHG E\ \RX RU
DQRWKHU DJHQF\” KWWS ZZZ JR
JXOI FRP IDT SKS IDTB
Ü , GRQ×W NQRZ H[DFWO\ ZKDW P\ UHTXLUHPHQWV DUH &DQ
\RX KHOS PH” KWWS ZZZ JR
JXOI FRP IDT SKS IDTB
7KH ZHE VLWH ORRNV IDQWDVWLF
-DQH %HYDQ b&R)RXQGHU
,QILQLW\ %DE\ &DUH &OLQLF ‘XEDL 8$(
EORJ SKS
,VUDHO
-DSDQ
5(63216(6 72 Ù&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@Ú
3LQJEDFN (VWDG®VWLFDV \ WHQGHQFLDV GH &ULPHQ ‘LJLWDO _ *HHNV5RRP
KWWS JHHNVURRP FRP HVWDGLVWLFDV \ WHQGHQFLDV GH FULPHQ GLJLWDO
3LQJEDFN /D SUHYHQFL´Q GHO URER GH GDWRV SRU SDUWH GH ORV HPSOHDGRV
‘HOOHQ’LUHFWR
‘HOOHQ’LUHFWR &RPPXQLGDG GH ‘HOO KWWS HV FRPPXQLW\ GHOO FRP GHOO
EORJV GLUHFW GHOO E GLUHFW GHOO DUFKLYH OD SUHYHQFL Q GHO URER GH
GDWRV SRU SDUWH GH
ORV HPSOHDGRV DVS[
/($9($ 5(3/<
<RXU 1DPH
<RXU (PDLO
<RXU &RPPHQW
68%0,7
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ 3DJH RI
KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH -DQ
&\EHU &ULPH 6WDWLVWLFV DQG 7UHQGV >,QIRJUDSKLF@ 3DJH RI
KWWS ZZZ JR JXOI FRP EORJ F\EHU FULPH –DQ

ملحق رقم (٦)

عدد مستخدمي مواقع شبكات التواصل الإجتماعي في دول مجلس التعاون لدول الخليج العربية


عدد مستخدمي مواقع شبكات التواصل الاجتماعي
في دول مجلس التعاون(مايو ٢٠١٣) (بالآلاف)
6,000
5,000
4,000
3,000
2,000
1,000
-
346
64
123
792
225
225
480
39
153
680
74
255
5,354
1,900
968
3,419
401
1,350
البحرين
الكويت
عمان
قطر
السعودية
الامارات
فيسبوك
تويتر
لينكد إن
InfoGraphic
مركز الرياض للمعلومات والدراسات الاستشارية

ملحق رقم (٧)

إحصائية موقف التوقيع والتصديق والنفاذ
لاتفاقية مجلس أوربا للجريمة الاليكترونية
من ب ـ د

موقف التوقيع والتصديق والنفاذ
لاتفاقية مجلس أوربا للجريمة الاليكترونية

Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States

Opening for signature Entry into force
Place: Budapest
Date : 23/11/2001 Conditions: 5 Ratifications including at least 3 member States of the Council of Europe
Date : 1/7/2004
Status as of: 14/1/2015

Member States of the Council of Europe

Country	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra	23/4/2013									
Armenia	23/11/2001	12/10/2006	1/2/2007				X			
Austria	23/11/2001	13/6/2012	1/10/2012		X	X	X			
Azerbaijan	30/6/2008	15/3/2010	1/7/2010		X	X	X	X		
Belgium	23/11/2001	20/8/2012	1/12/2012		X	X	X			
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Croatia	23/11/2001	17/10/2002	1/7/2004				X			
Cyprus	23/11/2001	19/1/2005	1/5/2005				X			
Czech Republic	9/2/2005	22/8/2013	1/12/2013		X	X	X			
Denmark	22/4/2003	21/6/2005	1/10/2005		X		X	X		

Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Finland	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia	1/4/2008	6/6/2012	1/10/2012			X				
Germany	23/11/2001	9/3/2009	1/7/2009		X	X	X			
Greece	23/11/2001									
Hungary	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Iceland	30/11/2001	29/1/2007	1/5/2007		X		X			
Ireland	28/2/2002									
Italy	23/11/2001	5/6/2008	1/10/2008				X			
Latvia	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein	17/11/2008									
Lithuania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003	16/10/2014	1/2/2015				X			
Malta	17/1/2002	12/4/2012	1/8/2012			X				
Moldova	23/11/2001	12/5/2009	1/9/2009			X	X	X		
Monaco	2/5/2013									
Montenegro	7/4/2005	3/3/2010	1/7/2010	55	X		X			
Netherlands	23/11/2001	16/11/2006	1/3/2007				X	X		
Norway	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Poland	23/11/2001									
Portugal	23/11/2001	24/3/2010	1/7/2010			X	X			
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										

Serbia	7/4/2005	14/4/2009	1/8/2009	55			X			
Slovakia	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spain	23/11/2001	3/6/2010	1/10/2010			X	X			
Sweden	23/11/2001									
Switzerland	23/11/2001	21/9/2011	1/1/2012		X	X	X			
The former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Turkey	10/11/2010	29/9/2014	1/1/2015							
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
United Kingdom	23/11/2001	25/5/2011	1/9/2011		X		X			

Non-members of the Council of Europe

Country	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Argentina										
Australia		30/11/2012a	1/3/2013		X		X			
Canada	23/11/2001									
Chile										
Colombia										
Costa Rica										
Dominican Republic		7/2/2013 a	1/6/2013			X	X			
Israel										
Japan	23/11/2001	3/7/2012	1/11/2012		X	X	X			
Mauritius		15/11/2013a	1/3/2014				X			
Mexico										
Morocco										
Panama		5/3/2014 a	1/7/2014				X			
Philippines										
Senegal										
South Africa	23/11/2001									
Tonga										
United States of America	23/11/2001	29/9/2006	1/1/2007		X	X	X			

Total number of signatures not followed by ratifications:	9
Total number of ratifications/accessions:	44

Notes:

(55) Date of signature by the state union of Serbia and Montenegro.

a: Accession - s: Signature without reservation as to ratification - su: Succession - r: Signature «ad referendum».

R.: Reservations - D.: Declarations - A.: Authorities - T.: Territorial Application - C.: Communication - O.: Objection.

Source : Treaty Office on http://conventions.coe.int – * Disclaimer

ملحق رقم (٨)

قائمة الترتيب الأمني السيبراني العالمي

للدول لعام ٢٠١٤

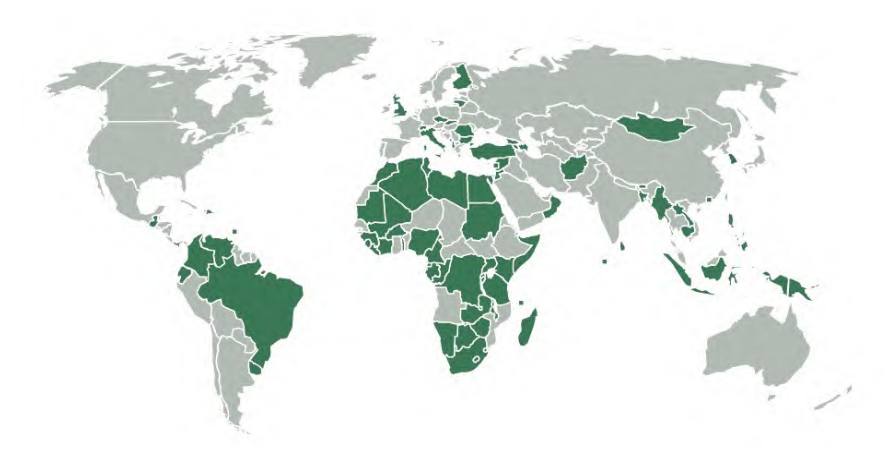
من ب ـ ح

قائمة الترتيب الأمني السيبراني العالمي للدول لعام ٢٠١٤

Global Cybersecurity Index

The Global Cybersecurity Index (GCI) is an ITU-ABIresearch joint project to rank the cybersecurity capabilities of nation states. Cybersecurity has a wide field of application that cuts across many industries and sectors. Each country's level of development will therefore be analyzed within five categories: Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation.

The final results for 2014 has been announced at ITU Telecom World›14, Doha on 9 December. Please see White Paper from ITU- ABIResearch.



Goals:

- Promote government strategies at a national level
- Drive implementation efforts across industries and sectors
- Integrate security into the core of technological progress
- Foster a global culture of cybersecurity

The GCI project finds its basis in the current mandate of the ITU and the related projects and activities of the BDT:

- WSIS Action Line C5 Building confidence and security in the use of ICTs
- ITU Plenipotentiary Resolutions (Guadalajara, 2010): 130, 174,179,181
- ITU WTDC Resolutions (Hyderabad, 2010): 45, 67, 69
- ITU WTSA Resolutions (Dubai, 2012) : 50, 52, 58.

Global 2014 results

Many countries share the same ranking which indicates that they have the same level of readiness. The index has a low level of granularity since it aims at capturing the cybersecurity preparedness of country and NOT its detailed vulnerabilities.

Country	Index	Global Rank
United States of America*	0.824	**1**
Canada*	0.794	**2**
Australia*	0.765	**3**
Malaysia	0.765	**3**
Oman	0.765	**3**
New Zealand*	0.735	**4**
Norway*	0.735	**4**
Brazil	0.706	**5**
Estonia*	0.706	**5**
Germany*	0.706	**5**
India*	0.706	**5**
Japan*	0.706	**5**
Republic of Korea	0.706	**5**
United Kingdom	0.706	**5**
Austria*	0.676	**6**
Hungary*	0.676	**6**
Israel*	0.676	**6**
Netherlands*	0.676	**6**
Singapore	0.676	**6**
Latvia*	0.647	**7**
Sweden*	0.647	**7**
Turkey	0.647	**7**
Hong Kong	0.618	**8**
Finland	0.618	**8**
Qatar	0.618	**8**
Slovakia	0.618	**8**
Uruguay	0.618	**8**
Colombia	0.588	**9**
Denmark*	0.588	**9**

Egypt	0.588	9
France*	0.588	9
Mauritius	0.588	9
Spain*	0.588	9
Italy	0.559	10
Morocco	0.559	10
Uganda	0.559	10
Azerbaijan	0.529	11
Poland*	0.529	11
Rwanda	0.529	11
Tunisia	0.529	11
Czech Republic	0.500	12
Georgia	0.500	12
Russia*	0.500	12
Indonesia	0.471	13
Luxembourg*	0.471	13
Romania	0.471	13
Belgium*	0.441	14
Bulgaria	0.441	14
China*	0.441	14
Lithuania	0.441	14
Nigeria	0.441	14
Sudan	0.441	14
Argentina*	0.412	15
Cameroon	0.412	15
Croatia	0.412	15
Kenya	0.412	15
Mongolia	0.412	15
Sri Lanka	0.412	15
Thailand*	0.412	15
Brunei Darussalam	0.382	16
Chile*	0.382	16
Moldova*	0.382	16
Montenegro	0.382	16
Myanmar	0.382	16
South Africa	0.382	16
Costa Rica*	0.353	17
Ecuador	0.353	17
Malta*	0.353	17

Philippines	0.353	17
Switzerland	0.353	17
Ukraine*	0.353	17
United Arab Emirates*	0.353	17
Burkina Faso	0.324	18
Mexico*	0.324	18
Peru*	0.324	18
Viet Nam*	0.324	18
Bahrain	0.294	19
Bangladesh	0.294	19
Cyprus*	0.294	19
Ghana*	0.294	19
Iran *	0.294	19
Libya	0.294	19
Panama	0.294	19
Portugal*	0.294	19
Saudi Arabia*	0.294	19
Afghanistan	0.265	20
Serbia	0.265	20
Togo	0.265	20
Cote d'Ivoire	0.235	21
Jamaica*	0.235	21
Albania	0.206	22
El Salvador*	0.206	22
Greece*	0.206	22
Guatemala	0.206	22
Iceland*	0.206	22
Ireland*	0.206	22
Jordan	0.206	22
Liberia	0.206	22
Paraguay*	0.206	22
Tanzania	0.206	22
Trinidad and Tobago	0.206	22
Venezuela	0.206	22
Algeria	0.176	23
Armenia	0.176	23
Barbados	0.176	23
Belarus*	0.176	23
Belize*	0.176	23

Benin*	0.176	23
Bosnia and Herzegovina	0.176	23
Botswana	0.176	23
Kazakhstan*	0.176	23
Malawi	0.176	23
Pakistan*	0.176	23
Samoa	0.176	23
Senegal*	0.176	23
Slovenia*	0.176	23
Syria	0.176	23
Bahamas*	0.147	24
Mauritania*	0.147	24
Nicaragua*	0.147	24
Saint Kitts and Nevis	0.147	24
State of Palestine*	0.147	24
Tajikistan*	0.147	24
Macedonia*	0.147	24
Uzbekistan*	0.147	24
Vanuatu	0.147	24
Zambia	0.147	24
Antigua and Barbuda*	0.118	25
Bhutan	0.118	25
Bolivia *	0.118	25
Burundi	0.118	25
Cambodia	0.118	25
Dominican Republic	0.118	25
Grenada	0.118	25
Guyana*	0.118	25
Kyrgyzstan*	0.118	25
Liechtenstein*	0.118	25
Micronesia	0.118	25
Nepal*	0.118	25
Papua New Guinea	0.118	25
Saint Lucia*	0.118	25
Seychelles*	0.118	25
Suriname*	0.118	25
Angola*	0.088	26
Gambia	0.088	26
Kiribati	0.088	26

Lebanon	0.088	26
Madagascar	0.088	26
Maldives	0.088	26
Mali	0.088	26
Monaco*	0.088	26
Niger*	0.088	26
South Sudan*	0.088	26
Tonga	0.088	26
Turkmenistan*	0.088	26
Zimbabwe	0.088	26
Andorra*	0.059	27
Congo	0.059	27
Djibouti	0.059	27
Dominica*	0.059	27
Fiji	0.059	27
Haiti*	0.059	27
Kuwait*	0.059	27
Lao	0.059	27
Mozambique*	0.059	27
Sao Tome and Principe	0.059	27
Sierra Leone	0.059	27
Swaziland	0.059	27
Tuvalu	0.059	27
Yemen*	0.059	27
Cape Verde	0.029	28
Chad*	0.029	28
Comoros	0.029	28
Cuba*	0.029	28
Democratic Republic of the Congo	0.029	28
Eritrea*	0.029	28
Ethiopia*	0.029	28
Gabon	0.029	28
Guinea	0.029	28
Guinea-Bissau*	0.029	28
Iraq*	0.029	28
Nauru	0.029	28
Palau*	0.029	28
Solomon Islands	0.029	28
Somalia	0.029	28

Central African Republic*	0.000	29
Democratic People's Republic of Korea*	0.000	29
Equatorial Guinea*	0.000	29
Honduras*	0.000	29
Lesotho	0.000	29
Marshall Islands	0.000	29
Namibia	0.000	29
Saint Vincent and the Grenadines	0.000	29
Timor-Leste*	0.000	29
		(Source : ABI Research)

ملحق رقم (٩)

قائمة بأسماء مراكز الاستجابة لطوارئ الحاسب الآلي

حول العالم

من ب ـ ط

قائمة بأسماء مراكز الاستجابة لطوارئ الحاسب الآلي حول العالم
Computer Emergency Response Team (CERTs)

CMU
SEI
CERT Division
Digital Library
Blogs
SEI Blog
CERT Blogs
أعلى النموذج
What are y
أسفل النموذج
CERT Menu
Work Areas
Welcome to CERT
Cyber Risk and Resilience Management
Cybersecurity Engineering
Digital Intelligence and Investigation
Incident Management
Insider Threat
Network Situational Awareness
Secure Coding
Vulnerability Analysis
New Publications
Blacklist Ecosystem Analysis Update: 2014
Predicting Software Assurance Using Quality and Reliability Measures
Regional Use of Social Networking Tools
Domain Parking: Not as Malicious as Expected
Pattern-Based Design of Insider Threat Programs
About CERT



Our mission at the CERT Division is to anticipate and solve the nation's .cybersecurity challenges
Learn more
Engage with Us
Training
CERT Training Courses
Curricula
Cyber Workforce Development
About Us
News
Careers
Information for
Researchers
Developers
System Administrators
Managers
Educators
Law Enforcement
Home
Incident Management
National CSIRTs
List of National CSIRTs
Share
Email
Print
Overview
Research
Publications
Case Studies
Products & Services
National CSIRTs
Annual Meeting
CSIRT Development

List of National CSIRTs

The following CSIRTs have responsibility for an economy or a country. This is complete to the best of our knowledge. Please contact us if any entries need .to be corrected or updated

أعلى النموذج

Abbreviation	Name	Country	Website	CFGRIDROWINDEX
DZ-CERT	Algerian Computer Emergency Response Team	Algeria	View	1
aeCERT	Arab Emirates Computer Emergency Response Team	United Arab Emirates	View	2
GovCERT.AT	Austrian Government Computer Emergency Response Team	Austria	View	3
CERT.GOV.AZ	Azerbaijan Government CERT	Azerbaijan	View	4
bdCERT	Bangladesh Computer Emergency Response Team	Bangladesh	View	5
BruCERT	Brunei Computer Emergency Response Team	Brunei Darussalam	View	6
CERT Bulgaria	Bulgarian Computer Security Incidents Response Team	Bulgaria	View	7
CCIRC	Canadian Cyber Incident Response Center	Canada	View	8
CARICERT	Caribbean CERT	Curacao	View	9
CTIR Gov	Center for the Treatment of Security Incidents on Computer Networks	Brazil	View	10
GovCERT.DK	Centre for Cyber Security	Denmark	View	11

KrCERT/CC	CERT Coordination Center of Korea	Korea South	View	12
CERT.PL	CERT Polska	Poland	View	13
CERT-SE	CERT-SE	Sweden	View	14
CERT-UK	CERT-UK National Computer Emergency Response Team	United Kingdom	View	15
CLCERT	Chilean Computer Emergency Response Team	Chile	View	16
CIRT.BF	CIRT Burkina Faso	Burkina Faso	View	17
colCERT	colCERT	Colombia	View	18
CERT AM	Computer Emergency Response Team Armenia	Armenia	View	19
CERT Australia	Computer Emergency Response Team Australia	Australia	View	20
CERT.br	Computer Emergency Response Team Brazil	Brazil	View	21
CERT-Bund	Computer Emergency Response Team - CERT-Bund	Germany	View	22
GovCertUK	Computer Emergency Response Team (CERT) for UK Government	United Kingdom	View	23
CERT-EE	Computer Emergency Response Team Estonia	Estonia	View	24
CERT-EU	Computer Emergency Response Team European Union	European Union	View	25
CERT.GOV.GE	Computer Emergency Response Team-Georgia	Georgia	View	26
CERT-IS	Computer Emergency Response Team Iceland	Iceland	View	27

CERT-MX	Computer Emergency Response Team Mexico	Mexico	View	28
CERT-Hungary	Computer Emergency Response Team of Hungary	Hungary	View	29
CERT-UA	Computer Emergency Response Team of Ukraine	Ukraine	View	30
CERT.PT	Computer Emergency Response Team Portugal	Portugal	View	31
CERT-RO	Computer Emergency Response Team Romania	Romania	View	32
CERT-SA	Computer Emergency Response Team Saudi Arabia	Saudi Arabia	View	33
CIRCL	Computer Incident Response Center Luxembourg	Luxembourg	View	34
CSIRT.CZ	Computer Security Incident Response Team of the Czech Republic	Czech Republic	View	35
CSIRT Panama	Computer Security Incident Response Team Panama	Panama	View	36
CSIRT.SK	Computer Security Incident Response Team Slovakia	Slovakia	View	37
CI-CERT	Cote d'Ivoire Computer Emergency Response Team	Cote DIvoire Ivory Coast	View	38
HR-CERT	Croatian National Computer Emergency Response Team	Croatia Hrvatska	View	39

CCN-CERT	Cryptology National Center Computer Emergency Response Team	Spain	View	40
EcuCERT	Ecuador CERT	Ecuador	View	41
EG-CERT	Egyptian CERT	Egypt	View	42
CERT-Py	Equipo de Respuesta ante Incidentes Ciberneticos	Paraguay	View	43
CERT-FR	French Government CSIRT	France	View	44
CERT-GH	Ghana National CERT	Ghana	View	45
GOV-CERT.RU	Gov-CERT.RU	Russia	View	46
GOVCERT.LU	Governmental Computer Emergency Response Team Luxembourg	Luxembourg	View	47
GovCERT.CZ	Government CERT of the Czech Republic	Czech Republic	View	48
HKCERT	Hong Kong Computer Emergency Response Coordination Centre	Hong Kong	View	49
CERTuy	Incident Response Center of Information Security Uruguay	Uruguay	View	50
CERT-IN	Indian Computer Emergency Response Team	India	View	51
ID-SIRTII/CC	Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center	Indonesia	View	52

CERT.LV	Information Technologies Security Incidents Response Institution Latvia	Latvia	View	53
CERTCC MAHER	Iran Computer Emergency Response Team/ Coordination Center	Iran	View	54
CERTGOVIL	Israel Governmental Computer Emergency Response Team	Israel	View	55
JPCERT/CC	Japan Computer Emergency Response Team	Japan	View	56
KZ-CERT	Kazakhstan CERT	Kazakhstan	View	57
KE-CIRT/CC	Kenya Computer Incident Response Team Coordination Centre	Kenya	View	58
KN-CERT	Korea National Computer Emergency Response Team	Korea South	View	59
LaoCERT	Lao Computer Emergency Response Team	Laos	View	60
CERT-LT	Lithuanian National Computer Emergency Response Team	Lithuania	View	61
MOCERT	Macau Computer Emergency Response Team - Coordination Centre	Macau	View	62
MyCERT	Malaysian Computer Emergency Response Team	Malaysia	View	63
CSIRTMalta	Malta National CSIRT	Malta	View	64

CERT-MU	Mauritian National Computer Security Incident Response Team	Mauritius	View	65
CIRT.ME	Montenegro Computer Incident Response Team	Montenegro	View	66
maCERT	Moroccan National Computer Emergency Response Team	Morocco		67
mmCERT	Myanmar Computer Emergency Response Team	Myanmar	View	68
CamCERT	National Cambodia Computer Emergency Response Team	Cambodia	View	69
NISC	National Center of Incident Readiness and Strategy for Cybersecurity	Japan	View	70
CERT.at	National Computer Emergency Response Team of Austria	Austria	View	71

أسفل النموذج

Visit the National CSIRT Wiki
The National CSIRT wiki provides easy access to materials of interest to CSIRTs with national responsibility.
Visit the National CSIRT wiki

Learn from Our Experts
John Haller and Jeff Carpenter discuss how a national CSIRT is essential for protecting national and economic security.
Listen to the podcast
Recommended Resources
Steps for Creating National CSIRTs
Related Areas of Work



Digital Intelligence and Investigation

The Digital Intelligence and Investigation Directorate (DIID) develops technologies, capabilities, and practices that organizations can use to develop incident response capabilities and facilitate incident investigations.



Insider Threat

The CERT Insider Threat Center conducts empirical research and analysis to develop and establish socio-technical solutions to combat insider cyber threats.



Network Situational Awareness

The Network Situational Awareness group has analyzed hundreds of cases of malicious activity on large, enterprise-scale networks to develop tools and approaches that help organizations defend their networks from potential attack.



Vulnerability Analysis

The Vulnerability Analysis team helps engineers reduce security risks posed by software vulnerabilities. The team addresses vulnerabilities in software being developed as well as in software already deployed.

Work Areas

Cyber Risk and Resilience Management

Cybersecurity Engineering

Digital Intelligence and Investigation

Incident Management

Insider Threat
Network Situational Awareness
Secure Coding
Vulnerability Analysis
Workforce Development
CERT Training Courses
Curricula
Cyber Workforce Development
Blogs
CERT/CC Blog
Insider Threat Blog
SEI Blog
Information for
Researchers
Developers
System Administrators
Managers
Educators
Law Enforcement
SEI Resources
Digital Library
Events
Engage with Us
About Us
News
Careers
Legal
Terms of Use
Privacy Statement
Intellectual Property
Connect with Us
RSS
Twitter
Linked In
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
U.S.A.
412-268-5800
Contact Us